NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE SIGNIFICANCE OF CONSEQUENCE ASSESSMENT APPLIED TO THE RISK BASED APPROACH OF HOMELAND SECURITY

by:

Richard B. Proctor

March 2008

Thesis Advisor:	Robert Bach
Second Reader:	Michael Chumer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE The Significance of Consequence Assessment Applied to the Risk Based Approach of Homeland Security	5. FUNDING NUMBERS
6. AUTHOR(S) Richard B. Proctor	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is to challenge the risk based approach of homeland security practice to elevate the significance of consequence during the Homeland Security risk assessment process. The consequence variable must be afforded an equal to or greater value similar to threat and vulnerability. In doing so, local homeland security policies can be focused towards consequence mitigation when planning and determining how to reduce risk within a designated jurisdiction.

Today's emergency preparedness risk environment has become increasingly more severe and complex, especially at the local level. The management of that risk is a fundamental requirement of local government which is expected to identify and anticipate areas of vulnerability and set in place a cohesive strategy across all disciplines to mitigate, reduce and eliminate these risks. The problem with this expectation is that federal guidance documents have a deliberate bias toward short term objectives which undermines a local government's long term commitment to the people it serves. Local agencies must be able to respond to emergencies in a way that minimizes the number of casualties or injuries during an incident that threatens members of their community and maintains services until the situation returns to normal.

14. SUBJECT TERMS Consequences, Consequence Assessment, Culture of Preparedness, Preparedness, Resilience, Risk, Risk Management, Threat, Vulnerability	15. NUMBER OF PAGES 91
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE SIGNIFICANCE OF CONSEQUENCE ASSESSMENT APPLIED TO THE RISK BASED APPROACH OF HOMELAND SECURITY

Richard B. Proctor
Civilian, Health Officer
B.A., Washington and Lee University, 1972
M.S., New Jersey Institute of Technology, 1997

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2008**

Author: Richard B. Proctor

Approved by: Robert Bach, Ph.D.
Thesis Advisor

Michael Chumer, Ph.D.
Second Reader

Harold A. Trinkunas
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to challenge the risk based approach of homeland security practice to elevate the significance of consequence during the Homeland Security risk assessment process. The consequence variable must be afforded an equal to or greater value similar to threat and vulnerability. In doing so, local homeland security policies can be focused towards consequence mitigation when planning and determining how to reduce risk within a designated jurisdiction.

Today's emergency preparedness risk environment has become increasingly more severe and complex, especially at the local level. The management of that risk is a fundamental requirement of local government which is expected to identify and anticipate areas of vulnerability and set in place a cohesive strategy across all disciplines to mitigate, reduce and eliminate these risks. The problem with this expectation is that federal guidance documents have a deliberate bias toward short term objectives which undermines a local government's long term commitment to the people it serves. Local agencies must be able to respond to emergencies in a way that minimizes the number of casualties or injuries during an incident that threatens members of their community and maintains services until the situation returns to normal.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. PROBLEM STATEMENT 1
B. IS IT POSSIBLE TO PROTECT OUR HOMELAND? 4

II. ELEMENTS OF RISK ASSESSMENT 9
A. MEASURING RISK 9
1. Threat 11
2. Vulnerability 12
3. Consequence 13
B. RISK APPLIED TO INDUSTRY AND BUSINESS 18
C. RISK MODELS 19
1. Natural Disaster Models 19
2. Terrorist Attack Models 20

III. THE FLAWED SPENDING PROCESS 25
A. HOMELAND SECURITY GRANT PROGRAM (HSGP) AND URBAN AREA SECURITY INITIATIVE (UASI) 25
B. CHALLENGING THE THREAT ASSUMPTION 29
C. RANDOM AUDITS 30

IV. CONSEQUENCE ASSESSMENT 35
A. FAILURE TO UNDERSTAND 35
B. FEDERAL GUIDANCE ON CONSEQUENCE ASSESSMENT 37
C. CONSEQUENCE OF MEGA-CATASTROPHES 42
1. Taking Consequences Seriously 45
D. ELEMENTS OF CONSEQUENCE 47

V. CULTURE OF PREPAREDNESS 53
A. POST 911 RESPONDER 53
B. BLACK SWAN PHENOMENON 58
C. BUILDING RESILIENCE 59

VI. CONCLUSION 63
A. RECOMMENDATIONS 66
B. COMMENTARY 66

LIST OF REFERENCES 69

INITIAL DISTRIBUTION LIST 75

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. DHS Risk Assessment Methodology for Fiscal Year 2007 UASI Funding Note: DIB is Defense Industrial Base. 17

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS/ACRONYMS

CDC	Centers for Disease Control
CHDS	Center of Homeland Security and Defense
CI/KR	Critical Infrastructure/Key Resources
DHS	Department of Homeland Security
EOC	Emergency Operation Centers
ESF	Emergency Support Function
FEMA	Federal Emergency Management Association
HAZUS-MH	Hazards U.S. Multi-Hazard
HLS	Homeland Security
HSGP	Homeland Security Grant Process
MBVA	Model Based Vulnerability Assessment
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NOAA	National Oceanographic and Air Administration
NPS	National Planning Scenarios
R = f (C, V, T)	Risk equals the Function of Consequence, Vulnerability and Threat
RMS	Risk Management Solutions
TCL	Target Capabilities List
UASI	Urban Areas Security Initiative
UCR	Usual and Customary Rates
UTL	Universal Target List
VCF	Victim Compensation Fund

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis would not have been possible without the help, support, and guidance of many individuals. First, I would like to thank Mayor James J. Kennedy. He is more than a good friend and without his support, I would not have had this extraordinary educational opportunity.

I gratefully acknowledge the faculty and staff of CHDS for their dedication and commitment to our education and to homeland security. Special thanks to Bill Pelfrey, Chris Bellavita, Bob Bach, Lauren Wollman and Greta Marlatt, each of whom has played a special role in making my experience at CHDS a great one. I would also like to thank the outstanding individuals of Cohort 0603-0604. I learned so much from them and I am proud to have been part of such an esteemed group of homeland security leaders.

Special thanks go to my Thesis advisor Bob Bach who guided me as I struggled to define and refine my thesis topic. His patience, direction and support through the tedious procession of drafts kept me on course despite my best efforts to wander off into the weeds. Thanks also go to my Second Reader Michael Chumer from the New Jersey Institute of Technology. His enthusiasm and support were motivational. Mike never let up with his encouragement. His dedication to Homeland Security is infectious

Finally, I am indebted to Denise Santiago, a graduate of the Center for Homeland Defense and Security, my guide, my inspiration but most importantly, my soul mate. I could not have succeeded in this program without her unequivocal support. This thesis would not have been written without her. She pushed, pulled and, at the end, dragged me forward through every obstacle. Denise's friendship, support and love are my most precious gift and I love her for it.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

> It's totally wiped out. ... It's devastating; it's got to be doubly devastating on the ground.
>
> –President Bush, turning to his aides while surveying Hurricane Katrina flood damage from Air Force One, August 31, 2005

The purpose of this thesis is to challenge the risk-based approach of homeland security practice and to elevate the significance of consequence during the Homeland Security risk assessment process. The consequence variable must be afforded a value equal to or greater than threat and vulnerability. In doing so, local homeland security policies can be focused towards consequence mitigation when planning and determining how to reduce risk within a designated jurisdiction.

Today's emergency preparedness risk environment has become increasingly severe and complex, especially at the local level. The management of that risk is a fundamental requirement of local government, which is expected to identify and anticipate areas of vulnerability, and set in place a cohesive strategy across all disciplines to mitigate, reduce and eliminate these risks. The problem with this expectation is that the same federal guidance documents are being used at the federal, state and local level as officials embark on similar, but very different, homeland security missions. A review of these documents will reveal a deliberate bias toward short-term objectives which undermines a local government's long term commitment to the people it serves. Local agencies must be able to respond to emergencies in a way that minimizes the number of casualties or injuries during an incident that threatens members of their community, and maintain services until the situation returns to normal.

Various emergency response disciplines interpret the numerous Homeland Security federal guidance documents in different ways in order to craft a plan to protect the public. In April 2005, the Department of Homeland Security (DHS) adopted a risk-based approach allocating Homeland Security (HLS) funding in identifying critical infrastructure. The problem with the approach is that local agencies are overwhelmed and intimidated in their preparedness efforts when identifying how and which elements of critical infrastructure within their communities to protect. Another problem with the approach is that, as local homeland security funding is allocated, vulnerability and threat factors far outweigh the significance of consequence when assessing the risk. If we as first responders ignore lessons learned, either from consequence assessments, scenario exercises or real time events, the public will lose trust and question our continued existence. New Orleans is a perfect example, because the probable consequences of a catastrophic hurricane were well known to emergency response planners, yet they failed to prepare.

Homeland Security grant funds – specifically related to the Homeland Security Grant Program (HSGP) and Urban Areas Security Initiative (UASI) – add to these problems because they are utilized for defensive measures. When disbursed to local agencies, the resulting funded programs tend to protect various targets perceived locally as valuable but which may be less significant from a broader national or cross-jurisdictional perspective. For example, the decentralized strategy has local governments often attempting to defend individual assets within a strongly networked critical infrastructure. As a result, federal grant dollars are encouraging local governments to spend in areas that represent the least effective strategy and which may even be counterproductive to the homeland security mission. Contributing to problems related to the allocation of funds is the problem that local governments have in managing grants using the current risk based approach in community preparedness efforts.

The National Infrastructure Protection Plan (NIPP) best defines **R**isk as "a **f**unction of **c**onsequence, **v**ulnerability, and **t**hreat: **R = f (C, V, T)**."[1] In this equation R = Risk, C = Consequence, V = Vulnerability and T = Threat. Despite the vagueness of the risk based approach concept, policy makers and stakeholders in every state and local jurisdiction in this country are expected to conform to federal guidance documents and utilize the risk assessment formula as fundamental in their preparedness efforts to prevent, respond to and recover from a possible attack or natural disaster. The approach is based on three criteria: 1) threat assessment, 2) vulnerability of a target and 3) consequence of a terrorist attack. According to the 2007 DHS Risk Assessment Methodology for the UASI Region, there is heightened priority and focus of threat and vulnerability when assessing and interpreting risk. Consequence, as identified in the same matrix, is not considered equally and is under represented in the risk analysis process. Locally, we cannot calculate and then act upon those calculations of risk unless and until we have a thorough understanding and awareness in measuring the impact of consequence. Local and state governments are probably best suited to calculate consequence in their area because of their extensive local situational awareness and boots on the ground expertise.

The consequence variable must be evaluated independently of threat and vulnerability. Currently, it is not. The result has a negative impact during the planning process because factors such as demographics, economics and social issues will be ignored, which prevents a complete and thorough consequence assessment. Without completely assessing the economic, human, housing and social costs of an attack or natural disaster, there is no way to accurately measure whether or not HLS efforts have reduced risk. Therefore, in order to plan, prepare and balance vulnerability and threat reduction with effective consequence reduction, it is important that local stakeholders have a thorough

[1] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2006), https://www.hsdl.org/homesec/docs/dhs/nps23-062906-01.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008), 35.

understanding of the full extent of the consequences. If used properly, an effective preparedness strategy can then be determined, and the ability to build a resilient community will be strengthened.

B. IS IT POSSIBLE TO PROTECT OUR HOMELAND?

The purpose of the National Strategy for Homeland Security is to guide and unify the country's efforts to achieve four goals: 1) Prevent and disrupt terrorist attacks; 2) Protect the American people, our critical infrastructure, and key resources; 3) Respond to and recover from incidents that do occur; and, 4) Continue to strengthen the foundation to ensure our long-term success.[2]

DHS further stresses "our first and most solemn obligation is to protect the American people. The *National Strategy for Homeland Security* will guide our Nation as we honor this commitment and achieve a more secure Homeland that sustains our way of life as a free, prosperous, and welcoming America."[3]

Accomplishing this massive task requires homeland protection to utilize various methods such as prevention, defense, mitigation, or enhanced response capability. In each method, risk reduction is accomplished by applying a different approach and acting on a different set of variables. Threat reduction, for example, requires investment in preventive methods such as added intelligence gathering and surveillance. The problem is that most local governments have limited access to federal intelligence sources and minimal terrorist intelligence gathering capability. Vulnerability reduction involves denying access to targets through target hardening or denying access to the means to launch an attack. Here the problem is that vulnerability reduction is target specific, yielding only incremental improvements in security. Consequence reduction is accomplished by providing redundant systems or enhanced planning and preparedness. The

---

[2] U.S. Homeland Security Council, *National Strategy for Homeland Security* (Washington, DC: The White House, 2007), http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed March 17, 2008), 1.

[3] Ibid.

advantage gained utilizing a consequence assessment method is the ability to apply an all-hazards framework. One can determine that a complete risk based approach requires an individual assessment of all three variables – threat, vulnerability and consequence when assessing the risk at the local level.

For example, Lewis points out that "one of the most fundamental assumptions made regarding the national strategy is that critical infrastructure protection is the responsibility of state and local government."[4] Therefore, local governments face a unique challenge in hometown security because limited manpower, minimal financial resources and a lack of expertise necessary in defending against a global terrorist threat are ongoing concerns impacting small town planning. With an abundance of potential terrorist targets across the nation, the threat is diluted and an "it can't happen here" attitude is developed. This attitude effectively reduces the priority of HLS concerns among local policy makers across the country because preparedness is not taken seriously. Complacency is already developing at the local level.

There continues to be an assumption shared by policy makers and DHS that local agencies can handle the monumental tasks of protecting each and every infrastructure component. Money cannot resolve the issue of preventing an attack, but because the risk based formula is not being used uniformly across each state, limited guidance has allowed agencies to spend as they deem appropriate--resulting at times in unnecessary, laughable and embarrassing purchases and procedures as states prioritize among identified risks and allocate their homeland security funds. Examples of unnecessary spending include the purchase of an air-conditioned garbage truck, segways, health club memberships, etc. The point is, spending grant dollars on items such as these items reduce our capacity in the mission to protect our homeland.

---

[4] Ted G. Lewis and Rudy Darken, "Potholes and Detours in the Road to Critical Infrastructure Protection Policy," *Homeland Security Affairs* I, no. 2 (Fall 2005), 1-11, http://www.hsaj.org/pages/volume1/issue2/pdfs/1.2.1.pdf (accessed August 29, 2007), 10.

On September 12, 2006, five years after the horrific World Trade Center attacks, Department of Homeland Security Secretary Chertoff appeared before Congress to say, “no matter how hard we may try, we cannot eliminate every possible threat to every individual in every place at every moment. And if we could, it would be at untenable cost to our liberty and our prosperity. Only by carefully assessing threats, vulnerabilities, and consequences, and prioritizing our resources, can we fully ensure the most practical and optimized protection for Americans and our nation.”[5] If we, as first responders, seriously agree with Secretary Chertoff’s message that because it is impossible and costly, and no matter how we try defending our communities, then we should begin planning by adopting an attitude that consequence assessment is a critical component in any effort to build the resilience of the nation. In doing so, we will begin to understand the direct relationship between a result and its cause, whether it is that of an attack or natural disaster.

First responders such as police officers, firefighters, public health officials and emergency medical providers realize that total *prevention* is impossible. Even if all terrorist attacks are prevented it is not possible to control nature, and therefore the nation remains vulnerable to natural disasters--the consequences of which can be more devastating than a manmade attack. Therefore, a local consequence reduction approach will result in risk reduction methodologies capable of working in an all-hazards framework. The benefit is dual use applications in promoting a culture of preparedness and, at the same time, building resilience at the community level.

The purpose of this thesis is to identify the need to enhance the significance of consequence assessment in local homeland security planning, wresting it out from under the dominance of threat and vulnerability calculations.

---

[5] Michael Chertoff, "Testimony of Secretary Michael Chertoff U.S. Department of Homeland Security before the Senate Committee on Homeland Security and Government Affairs," Department of Homeland Security, http://www.dhs.gov/xnews/testimony/testimony_1158336548990.shtm (accessed August 29, 2007), 2.

In Chapter II, I examine the elements of risk management and compare how the private sector, federal government and local officials view risk reduction. Chapter III provides an overview of how the risk-based approach is applied in distributing funds to local governments and how that method is failing from strategic, economic and practical viewpoints. Chapter IV describes consequences of a disaster in terms of preparedness and how federal guidance actually forces local governments to adopt short term; response oriented objectives rather than long term preparedness goals. Chapter V demonstrates how a comprehensive consequence assessment can assist local planners by revealing the need for a paradigm shift in the culture of preparedness necessary to build a resilient community. Chapter VI offers several conclusions and recommendations for enhancing the resilience of the nation, and ways to develop a culture of preparedness.

THIS PAGE INTENTIONALLY LEFT BLANK

II. ELEMENTS OF RISK ASSESSMENT

This chapter will discuss the three variables of the risk equation and evaluate the elements of a risk assessment to determine how risk can be measured. Applied to the business sector, an assertion is made that consequence reduction is a viable business option that improves business resilience. Current risk models are identified and the relevance of each to consequence assessment is discussed.

A. MEASURING RISK

Although risk is a pervasive theme in homeland security writings and strategies, there is no single official tool to assess risk in government documents. The problem is that risk is defined and used many different ways by agencies planning toward the next attack or disaster. In a 2004 Congressional Research Service document entitled *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences,* author John Moteff cites several definitions of risk used by different federal agencies. He observes that the terms vulnerability, threat and risk are integrated and used repeatedly within documents; never clearly defined, and simultaneously clouding the intent of what is being proposed or discussed.[6] The result of this confusion is that these terms continue to be used loosely in hearings, articles in the press, and other public discourse.

An example in the application of risk is defined in the National Infrastructure Protection Plan (NIPP) – that risk is "a measure of potential harm that encompasses threat, vulnerability, and consequence. In this context, risk is the potential for loss, damage, or disruption to the Nation's Critical

[6] John Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences* (Washington, DC: Congressional Research Service,[2004]), https://www.hsdl.org/homesec/docs/crs/nps17-100804-19.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008), 3.

Infrastructure/Key Resources (CI/KR) resulting from destruction, incapacitation, or exploitation during some future man-made or naturally occurring event."[7] Here the primary focus is on preventing system disruption rather then the consequence of a disruption during an incident. Ortwin Renn authored a white paper for the International Risk Governance Council that provides a framework for risk assessment and risk management strategies. Renn explains that risk always refers to a combination of two components: 1) the likelihood or chance of potential consequences, and 2) the severity of consequences of human activities, natural events or even a combination of both. Such consequences can be positive or negative, depending on the values people associate with them.[8] These distinctions are important when assessing consequences or developing risk management options because one favors vulnerability reduction and the other consequence reduction--both are very critical as planners identify risks.

In the RAND study *Guiding Resource Allocations Based on Terrorism Risk*; Henry Willis claims the risk formula "provides a clear mapping between risk and approaches to managing or reducing risk."[9] He continues to note that intelligence and active defense--*taking the fight to the enemy*--represents a prevention approach to risk management that focuses specifically on threats. "Managing risk through vulnerability reduction is a defensive tactic that includes increasing surveillance and detection, hardening targets, or other capabilities that might reduce the success of attempted attacks. Finally, managing risk through consequence reduction is a strategy that employs planning and preparedness to improve response and reduce the effects of damage through mitigation or

---

[7] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 35.

[8] Ortwin Renn, *Risk Governance: Towards an Integrative Approach* (Geneva, Switzerland: International Risk Governance Council, 2006), http://www.irgc.org/irgc/IMG/projects/IRGC_WP_No_1_Risk_Governance_(reprinted_version).pdf (accessed August 26, 2007).

[9] Henry H. Willis, "Guiding Resource Allocations Based on Terrorism Risk," *Risk Analysis* 27, no. 3 (June 2007), 597-606, 599.

compensation."[10] There is a specific reference to the idea that consequences can be reduced effectively by methods other than vulnerability reduction.

The perception of risk then lies in the eyes of the beholder, especially *when deciding what to protect*. For instance, Robert Ross, Deputy Director, Office of Comparative Studies in DHS' Science and Technology Directorate argues that risk, no matter how well founded, is in reality a mental and emotional construct rather than a physical reality. He says that risk has to do with feelings about a possible future that would be different than we would like or expect.[11] Therefore, the manner in which consequences are visualized will have a potent impact on how risks are perceived. Consequence is the variable that gives risk its emotional impact and continues to be portrayed in only one dimension. The following three variables-- 1) threat, 2) vulnerability and 3) consequence-- continue to define risk and the current use for allocation of the homeland security grant process.

1. Threat

Threat has been defined as "the likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk from terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary; in the context of natural disaster or accident, the likelihood is based on the probability of occurrence."[12] In the recent RAND study *Exploring Terrorist Targeting Preferences,* threat is evaluated and analyzed by possible motives for major worldwide terrorist attacks beginning from the 1993 World Trade Center bombing in New York to the 2004 Hilton Hotel bombing in Taba, Egypt. On the basis of past al Qaeda operations and statements it would appear that the group's target selection has been heavily influenced by three

[10] Willis, "Guiding Resource Allocations Based on Terrorism Risk," 599.

[11] Robert G. Ross, "Risk and Decision-Making in Homeland Security" (Baltimore, MD, Society for Risk Analysis Annual Meeting, December 3-6, 2006, 5.

[12] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 35.

motivations: 1) to coerce (unfriendly governments), 2) to damage economies and 3) to rally supporters and potential supporters.[13] Motive encompasses the relationship between the group's goals and its perception of the value of attacking a given target as a way of fostering these goals. Target selection, of course, is not the same as motive.

"Intent alone is insufficient to predict what will be attacked because feasibility must be taken into account."[14] Nor can motives be used alone as a reliable attack predictor. Terrorists must also have the capability to conduct an attack, although capability does not define what a group wants to do. Capability is a combination of resources, applied against a vulnerable target that fulfills the group's intentions at an acceptable cost. When assessing the risk, a simple and useful definition of threat is "the probability that a specific target is attacked in a specific way during a specified time period."[15] The continued problem with defining threat is that threat is a function of a series of unknown variables. If any variable equals zero then the threat remains zero as well. The only way to prevent terrorism is through intelligence. An effective intelligence gathering program can infiltrate and observe the actors who will carry out attacks; it can monitor the development of resources that build capability; and, it can maintain the situational awareness that is needed to preempt and stop terrorist attacks on any targets. Most local governments have limited access to federal intelligence sources and minimal terrorist intelligence-gathering capability.

2. Vulnerability

Vulnerability is defined by the NIPP as "the likelihood that a characteristic of, or flaw in - an asset, system, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or

---

[13] Martin C. Libicki, Peter Chalk and Melanie Sisson, *Exploring Terrorist Targeting Preferences* (Santa Monica, CA: Rand Corporation, 2007), http://www.rand.org/pubs/monographs/2007/RAND_MG483.pdf (accessed March 13, 2008), 95.

[14] Ibid., 3.

[15] Willis, *Guiding Resource Allocations Based on Terrorism Risk*, 598.

exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards."[16] Often seen as the probability that an attack of a given type will succeed, vulnerability commonly represents "the probability that damages occur, given a specific attack type, at a specific time, on a given target."[17] Damages may involve fatalities, injuries, property damage, or other consequences–-there is no limit. It is at this moment when the operative terminology becomes Critical Infrastructure Protection. Target hardening has become one of the primary counter terrorism strategies employed by state and local HLS professionals. Unfortunately, local HLS professionals in the quest for zero risk can mistakenly view vulnerability reduction as a preventive strategy, when in reality vulnerability reduction is purely a defensive posture, giving it a higher emphasis than it deserves. Vulnerability reduction is a defensive mode, and it would be a misnomer to consider it preventative. Gates, guns and gadgets defend specific assets from the enemy.

Vulnerability at the local government level should be viewed as an inability to maintain vital services. There are too many targets and not enough threats to attempt defending each asset. However, the measures taken to support victims of a chemical plant explosion are the same as a freight train wreck. The same can be argued for a bomb at a shopping center or a tornado through a town, or an influenza pandemic and a biological weapon. Locally, planners have to prepare for all types of hazards, and consequence assessments can identify preparedness gaps.

3. Consequence

Consequence, the last variable in the equation of the risk based formula has been categorized in ways such as economic; financial; environmental;

---

[16] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 35.

[17] Willis, "Guiding Resource Allocations Based on Terrorism Risk," 598.

technological, operational, health and safety; and, relevant to time.[18] Literature studying aspects of consequence exists in various disciplines concerned with risk or risk reduction. Lloyd Dixon and William Thompson both wrote articles that reviewed actual costs of the September 11th attacks. Robert Hartwig and Christopher Lewis wrote articles concerning the impacts on the insurance industry caused by terrorist attacks. Michael Moody and Janice Obuchowski wrote about business applications of risk reduction methods. Charles Meade and Roger Molander of RAND presented an analysis of a hypothetical nuclear attack on the Port of Long Beach, while Henry Willis, also of RAND, used an insurance industry risk assessment model to rank the risk to Urban Area Security Initiative regions. Vickie Bier applied game models and probability to compare different defender strategies in homeland security situations.

During the risk assessment process, however, limited effort goes into the process of quantifying consequence. There is a need to Identify and enumerate elements such as loss of lives; number/type of non-fatal injuries; medical costs; housing units lost; number of people requiring shelter, etc. This process is time–consuming, with numerous data sources outside the normal sphere of business for first responders. However, these elements are responsive to mitigation and could reduce consequences, if identified with proper planning. Three recent studies, each otherwise exceptionally well done, lack detail on the important measure of the impact of lives lost in a consequence assessment. First, a 2006 RAND study was conducted to consider the effects of a nuclear attack on the Port of Long Beach, CA.[19] While this study estimates the number of people killed in the attack, demonstrating that this type of assessment is both possible and feasible, it is framed solely in terms of dollars of economic and actuarial loss. A

[18] John Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences* (Washington, DC: Congressional Research Service, 2005), http://www.fas.org/sgp/crs/homesec/RL32561.pdf (accessed March 13, 2008), 5.

[19] Charles Meade and Roger C. Molander, *Considering the Effects of a Catastrophic Terrorist Attack* (Santa Monica, CA: Rand Center for Terrorism Risk Management Policy, 2006), http://www.rand.org/pubs/technical_reports/2006/RAND_TR391.pdf (accessed August 26, 2007).

second study conducted by RAND was to evaluate the consequences to the World Trade Center attacks. Here again, the study addressed loss in terms of compensation paid to the victims of the attacks. The classes of loss were applied to the following:

- *personal injury*: death, physical injury, environmental exposure injuries, emotional injuries, and workman's compensation
- *financial injuries*: income loss to workers and resident's, small business losses, business interruption and event cancellation, economic revitalization, environmental clean-up
- *property damage.*[20]

Lastly, in a 2002 study conducted by William C. Thompson, Jr., Comptroller of the City of New York, Mr. Thompson explored the unexpected expenses experienced by the city in terms of lost tax revenue, additional operational expenses and capital costs. In this study, unexpected loses are considered and an assessment of the lost wealth in both property and human potential is included, and also provides an estimate of the loss to the Gross City Product.[21] The sum of these studies incorporates a wide-ranging picture of the social and personal effects of consequences of a catastrophic terrorist attack, which can be used to begin to enumerate or catalog the classes of risk and begin to point out where data sets exist for further study. Unfortunately, it took the emotional impact of lives lost at the World Trade Center Terrorist attack as well as the natural disaster of Hurricane Katrina to force the homeland security mindset to begin thinking along the lines of increasing the application of consequence as a critical factor in the risk assessment equation. At the federal

[20] Lloyd Dixon and Rachel Kaganoff Stern, *Compensation for Losses from the 9/11 Attacks* (Santa Monica, CA: RAND Corporation, 2004), http://www.rand.org/pubs/monographs/2004/RAND_MG264.pdf (accessed August 29, 2007).

[21] William P. Thompson, Jr., *One Year Later: The Fiscal Impact of 9/11 on New York City* (New York, NY: City of New York, Office of Comptroller, 2002), http://www.comptroller.nyc.gov/bureaus/bud/reports/impact-9-11-year-later.pdf (accessed August 27, 2007).

level, however, the lessons learned from these tragedies and the knowledge we have gained from them have not significantly influenced the depth of DHS's utilization of consequences in risk assessments formula.

Figure 1 demonstrates the latest iteration of the consequence variable, illustrating its added weight in the 2007 Risk Based Approach formula. At first glance one will conclude that vulnerability and consequence equal 80 points and threat is 20 points – sounds good, right? Not really! The figure actually shows that vulnerability and consequence factors are comprised of four elements--two pure consequence factors of a population index and an economic index. But also included is a national infrastructure index that relates to vulnerability as well as a national security Index that relates to regional threat.[22] This is the very point of the thesis: that, although broken out to a degree, consequence is not measured in a fashion that facilitates discussion of any strategy other than vulnerability reduction. Local agencies are unable to seriously consider consequence as an equal part of the equation. This system becomes convoluted and further proves that consequence is not taken seriously, especially since this is the formula used for the 2007 DHS allocation matrix for Urban Area Security Initiative (UASI) Areas.

[22] U.S. Government Accountability Office, *Homeland Security Grants: Observations on Process DHS used to Allocate Funds to Selected Urban Areas* (Washington, DC: GAO, (2007), http://www.gao.gov/new.items/d07381r.pdf (accessed August 27, 2007), 6.

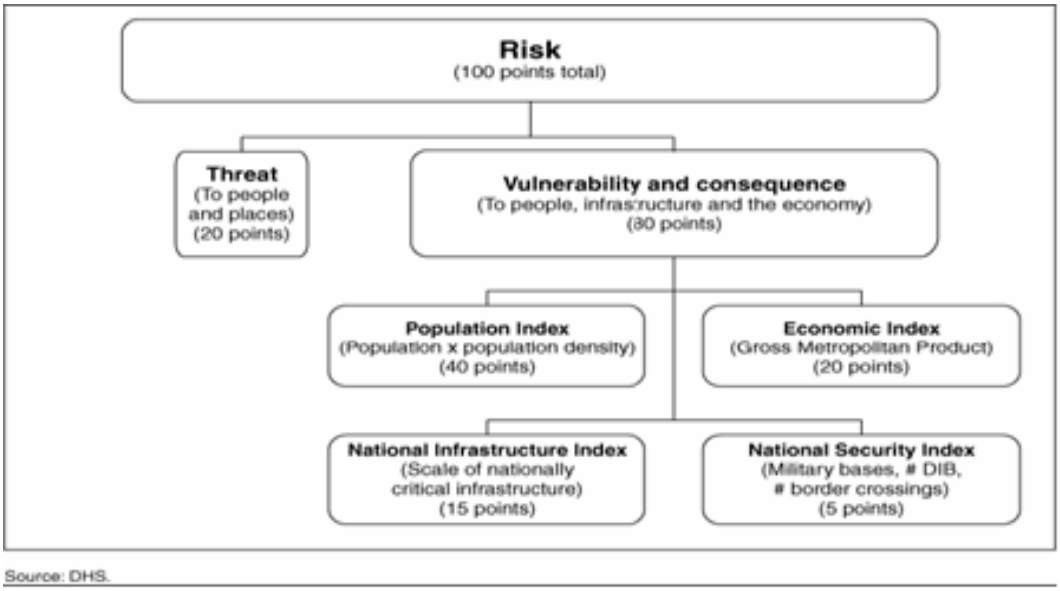

Figure 1. DHS Risk Assessment Methodology for Fiscal Year 2007 UASI Funding Note: DIB is Defense Industrial Base.[23]

Information on risk provides local, state, and federal homeland security leaders with the basis for understanding the trade-offs between the probability of an attack and its consequences as well as a metric (i.e., expected fatalities or property losses) for making decisions on prevention and protection actions. The ability to answer questions regarding attack-mode likelihood provides local homeland security officials with information concerning the types of attack for which they should prepare. Available targets, local characteristics and attractiveness to terrorists of particular attack modes vary from one city to another. Planning for each attack variant is time consuming and expensive for local government. Therefore, information on consequences provides local officials an understanding of what the effects of such attacks might be and identifies the common resources necessary to respond.[24]

---

[23] U.S. Government Accountability Office, *Homeland Security Grants: Observations on Process DHS used to Allocate Funds to Selected Urban Areas*, 6.

[24] Henry H. Willis and others, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection* (Santa Monica, CA: Rand Corporation, 2007), http://www.rand.org/pubs/technical_reports/2007/RAND_TR386.pdf (accessed March 13, 2008), Summary, xv.

B. RISK APPLIED TO INDUSTRY AND BUSINESS

Viewed by the insurance industry, risk is more concerned with economic loss–-specifically property loss and actuarial costs. The insurance industry concerns are expressed as the inability to assign economic responsibility for risk.[25] Consequence is viewed in dollar terms in order to value risk pools and/or risk portfolios so that financial exposure is also reduced. It is fair to conclude that their approach to risk management of terrorist threats is strictly to minimize financial liability and not to enumerate or define consequence related factors. Financial studies focus on disaster loss and cost reimbursement for recovery.

In his testimony before Congress, Christopher Lewis, Vice President of Alternate Market Solutions for the Hartford Financial Group, described the insurance dilemma by saying "the primary issue before the Congress with respect to managing the impact of terrorism on the U.S. economy is to identify the most efficient means to finance the risk of terrorism."[26] If true, this statement certainly supports the industry position that the random nature of terrorist attacks, the potentially catastrophic nature of an attack and the relatively small number of data sets prevent development of a reliable predictive rate model.[27] This underscores the problem that the insurance industry faces--determining how to build risk pools that will cover major attacks yet remain affordable to private sector clients. If the industry is unable to reasonably forecast where losses will occur and build risk pools capable of surviving the random terrorist attack without bankrupting the company or pricing premiums out of the reach of customers, they will seek protection from the federal government. Recent advances in consequence assessments evolve from firms who rate insurance industry

---

[25] Willis and others, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*

[26] Christopher M. Lewis, *Terrorism Threats and the Insurance Market*, July 25, 2006), 1, https://www.hsdl.org/homesec/docs/testimony/nps30-112806-05.pdf&code=fdcc9268909f5a990576e32d11c9f054 (accessed August 25, 2007), 1.

[27] Robert P. Hartwig, "The Cost of Terrorism: How Much Can We Afford?" (Philadelphia, PA, National Association of Business, Economics, 46th Annual Meeting, October 4, 2004, http://server.iii.org/yy_obj_data/binary/736851_1_0/tria.ppt (accessed August 29, 2007).

Catastrophe Funds, risk pools that are specifically designed to underwrite mega-catastrophes such as Hurricane Katrina. Here sophisticated modeling creates detailed forecasts of probabilities of a disaster and the financial consequences. These models have been used to good effect analyzing natural disasters of all types because of the amount of reliable data on these events.

C. RISK MODELS

DHS has developed baseline standards for assessing, analyzing, and combining the three specific components that make up risk, consequence, vulnerability, and threat[28], and yet strategies to reduce risk have primarily concentrated on risk assessments that stress the defensive tactic of vulnerability reduction. For vulnerabilities to be identified and reduced, state and local homeland security planners rely on risk assessment models applicable to their own jurisdiction. In his book *Critical Infrastructure Protection in Homeland Security,* Ted G. Lewis developed a model with high degrees of complexity and methodologies for allocating vulnerability reduction resources on a sector or system wide basis. The model is known as the Model Based Vulnerability Assessment (MBVA) approach in which risk is viewed as vulnerability times cost. Consequences, on the other hand, are framed in general terms - principally economic, but the true focus of this model is on fault reduction rather than consequence assessment.

1. Natural Disaster Models

The National Oceanographic and Air Administration (NOAA) and Federal Emergency Management Agency developed models applicable to natural disaster. The NOAA Earth System Research Laboratory maintains a library of weather and ocean system data sources that are available to modelers and forecasters as part of its Real Time Verification System. This information allows highly detailed forecasts and provides resources for prospective and

[28] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 36.

retrospective studies when planning for a natural disaster. FEMA's Hazards U.S. Multi-Hazard (HAZUS-MH) is a nationally applicable standardized methodology and software program that estimates potential losses from earthquakes, hurricane winds, and floods. Although natural disasters are difficult to plan for, "estimating losses is essential to decision-making at all levels of government, providing a basis for developing mitigation plans and policies, emergency preparedness, and response and recovery planning."[29] NOAA and FEMA models go further, to analyze risk by assessing potential loss mitigation strategies on the basis of 1) threat--based on historic storm tracks, weather patterns etc.; 2) vulnerability--based on historic event data; 3) capability, based upon storm or event projections; 4) and consequence--based on potential for human and financial loss. The ability to apply these variables consistently in the planning process is crucial as we attempt to reduce risk and capture loss data in the footprint of natural disasters.

As models are developed towards risk reductions, researchers are refining risk estimates for the insurance industry while consultants are improving risk assessment software - they are realizing the importance of consequence as a variable within their models, whether it is for terrorism, natural disasters or all-hazards planning. Provisions in modern building codes reflecting consideration of seismic effects on structures and standards for construction methods resistant to wind and water damage are examples of the private sector employing lessons learned from natural disasters. These are, in turn, used to influence government regulation and mandate mitigation strategies to reduce potential losses.

2. Terrorist Attack Models

Several modeling attempts have been developed, but the most recent impressive model applicable to consequence assessment is identified in a 2007 study called *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure*

[29] "HAZUS-MH Overview," FEMA, http://www.fema.gov/plan/prevent/hazus/hz_overview.shtm (accessed March 17, 2008).

Protection[30] developed by Risk Management Solutions (RMS) in which researchers utilize a Probabilistic Terrorism Risk Model. The importance of modeling terrorist attacks is:

> if the resources required to accomplish different attacks can be characterized, if some insight into terrorist capabilities can be collected, and if the consequences of different attacks can be related to terrorists' goals, then the full set of possible attacks could be reduced to only those for which the terrorists' capabilities meet or exceed the attack requirements and for which attack consequences correspond to their goals. The basic approach thus entails comparing terrorists' intentions, capabilities, and resources with the resource requirements and consequence estimates for various possible attacks in an attempt to constrain the range of probable attacks and, ultimately, to help guide intelligence analysis and surveillance efforts.[31]

The Probabilistic Terrorism Risk Model considers various target characteristics and attack methods to rank attack threat. The model attempts to take terrorist motives, resource needs and capabilities into account. The criticality of this model today relative to consequence assessment is fascinating, as it demonstrates how detailed consequence assessment will contribute to the planning stages when assessing risk. Not only can the RMS model assess various attack categories based on the threat such as biological, chemical, radiological, nuclear and explosive, but it identifies target type such as cultural icons, infrastructure sector, municipality or specific location. The versatility of this model is that it can be applied anywhere in the country. Of course, accuracy and specificity will increase as detailed local information is inserted into the model.

Agencies agree that the best method today to prevent terrorist attacks is through intelligence; the RMS model demonstrates capability to use intelligence information to provide an estimate of attack scenarios representing the greatest risk. By using risk analysis tools, such as the RMS model, raw intelligence can be

---

[30] Willis and others, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection.*

[31] Ibid., 45.

analyzed to help understand what attack modes meet terrorists' objectives in terms of consequences, required capabilities, and available skills and resources.[32] Companies continue to develop and modify risk models that provide highly detailed consequence pictures capable to build out risk pools to insure assets at risk from terrorism or natural disaster and, at the same time, provide homeland security applications. No doubt there is the need to improve consequence-modeling methodology to assist preparedness efforts,[33] and if utilized during the planning process, planners would have a greater understanding of the depth and reach of the effects of a given disaster.

This chapter began by looking at the three variables of the risk equation--how they are defined and how they are used. Each term has a different context for federal and local stakeholders. Threat, for instance, is a condition largely out of the purview of local officials. Vulnerability, however, has two contexts that relate to local government. Asset vulnerability has great importance if threat is uniform; however, we will see that this is not the case because terrorism risk is concentrated in a relatively few areas of the country. Therefore vulnerability should be viewed differently by local governments--not from a terrorist threat but from an all-hazards perspective. Consequences, on the other hand, are uniquely local and human in nature. Local officials have a vested interest in reducing casualties to incidents, yet the federal guidance largely ignores the human element of disaster consequences. These human elements are relatively well known thanks to the September 11th attacks and Hurricane Katrina; however, they are not weighted proportionally in federal guidance.

---

[32] Willis and others, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, 47.

[33] National Science and Technology Council, *Combating Terrorism: Research Priorities in the Social, Behavioral and Economic Sciences* (Washington, DC: Executive Office of the President, Office of Science and Technology Policy, 2004), http://www.ostp.gov/nstc/html/terror.pdf (accessed August 29, 2007).

Private industry has recognized the importance of accurately assessing consequences and mitigating their effects as a necessary and cost effective business processes. As part of the consequence assessment process government and industry have developed models that can be modified to homeland security purposes. Adaptation of these models could yield tools that are adaptable to each level of government by assessing risk from different perspectives. The private sector approach to risk assessment is a more useful construct for local governments. It focuses on looking at vulnerabilities and finding ways to mitigate losses.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE FLAWED SPENDING PROCESS

There is a strategic basis for the local role in critical infrastructure protection, but since programs are being funded through a federal grant allocation, the spending process is flawed down the chain of federal, state and local agencies. There remains an assumption that the country is under a uniform level of threat; however, this very threat assumption has been challenged--eroding the underlying principal of the HSGP and UASI grants. Grant management audits will be exposed to reveal numerous shortcomings in state management of homeland security funds.

A. HOMELAND SECURITY GRANT PROGRAM (HSGP) AND URBAN AREA SECURITY INITIATIVE (UASI)

In an effort to direct local homeland security strategies toward national strategy goals, the federal grant guidelines specify funding priorities that direct local officials to risk reduction activities on targets identified by one of the risk assessment tools promulgated by DHS and/or state Homeland Security strategies. Once again, these risk assessment tools are based on the formula mentioned earlier R = *f* (T, V, C). The benefit of this approach to critical infrastructure protection is that grant spending is directed to risk reduction outcomes. The problem today is that there is no requirement, methodology or evaluation tool to assess whether expenditures do lead to actual risk reductions, especially within the Homeland Security Grant Program (HSGP) and Urban Area Security Initiative (UASI) allocations. In fact, Ted Lewis states, "performing vulnerability and risk analysis of national assets at the local level will generally lead to waste and ineffective use of resources."[34] Negative publicity on ineffective use of resources will continue as long as agencies do not have metrics to measure risk reduction.

[34] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: John Wiley & Sons, Inc., 2006), 474.

Lewis' skepticism regarding the effectiveness of local homeland security spending and decisions concerning critical infrastructure vulnerability reduction stems from two uncertainties: 1) a lack of understanding of where the local measures fit in the overall infrastructure sector-wide risk picture and 2) what consequences, if any, the local measures have averted. This holds true, but to a slightly lesser extent, for federally funded measures to improve response capability, because guidance is still geared to the short term and incremental improvements. Unfortunately, the risk assessment tools do not encourage a comprehensive, empirical consequence assessment of an attack or natural disaster. Preparedness and mitigation efforts are hampered by the tunnel vision that results when consequence is portrayed simply as a dollar figure used to prioritize vulnerability reduction projects, without considering the full scope and nature of the impact of the disaster. The challenge is changing the mindset that defense is the single best option in every risk reduction situation. Risk management policies cannot truly manage risk without knowing the dynamics and costs of the consequences. HLS spending priorities continue to be set without complete understanding or awareness of consequences, costs of mitigation, or effectiveness of defensive measures. It is imperative that HLS planners begin to enumerate the many effects of terrorist attack and natural disaster that comprise the total range of disaster consequences.

UASI funds address the unique multi-disciplinary planning, operations, equipment, training, and exercise needs of high-threat, high-density urban areas. This program provides funding to high-risk urban areas based on risk and effectiveness.[35] The intent was to ensure that necessary funding for infrastructure protection was allocated throughout the country, distributed to county and local communities for various HLS projects, and expected to meet the mission statement and goals of the Department of Homeland Security. In 2005,

[35] U.S. Department of Homeland Security, *FY 2007 Homeland Security Grant Program* (Washington, DC: Department of Homeland Security, 2007), https://www.hsdl.org/homesec/docs/dhs/nps22-071807-01.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

the UASI program allocated $854 million to fifty UASI regions. In 2007, the same UASI program reduced both the allocation and the number of recipients by budgeting $746 million to forty-five (45) UASI regions. In the research of Vickie Bier, *Choosing What to Protect,* the decentralized strategy of funding multiple defenders to defend large numbers of assets is challenged. Several defensive strategies are evaluated, and Bier finds that defenders can only optimize expenditures based on the following conditions:

- there are a limited number of targets,
- a centralized defender (i.e., federal government) will more efficiently allocate resources than a de-centralized defender (i.e., state and local governments), and
- defending low value targets not only wastes resources but actually increases the likelihood that a higher value target will be attacked.

If applied to the real world homeland security strategy, troubling connotations would eventually result in the realization that we are employing the least effective method and strategy relative to the grant process. Actually, the strategy underlying the HSGP and UASI grant programs may actually be counterproductive to the homeland security mission.[36] A major problem for risk reduction using HSGP and UASI spending is that the funds are utilized for defensive measures on various targets perceived locally to be valuable but without reference to wider national or cross-jurisdictional priorities. If taken in this context there are–-for all practical purposes–-an unlimited number of assets of undetermined value in areas with unknown threat. “Spending too much on defense of assets that are not highly valuable hurts the defender in two ways — not only by wasting resources on defense of assets that are unlikely to be attacked in any case, but also by increasing the likelihood of a more valuable asset being attacked.”[37] Lewis’ assertion that infrastructure protection tasks relegated to local government generally lead to waste and ineffective use of

[36] Vicki M. Bier, "Choosing what to Protect," *Risk Analysis* 27, no. 3 (June 2007), 607-620.

[37] Ibid., 611.

resources is supported by the formula spending plan.[38] Current practices and spending are compelling evidence, and support Ms. Bier's argument that decentralized defenders will invest in defensive solutions that are either marginally effective or which deflect risk to another defender. The reality is that protecting low-risk targets can be harmful to overall security.[39]

Both HSGP and UASI spending reveals the need to quantify consequence scenarios so that parameters are established in order to measure the effectiveness of risk reduction measures. "DHS acknowledges the uncertainty of consequence values [used in the risk assessment model equation for the HSGP and UASI] used in the model, but does not know of available databases for consequence information for all asset-scenario pairs."[40] When RAND researchers analyzed the risk of terrorist attacks in UASI regions they recommended, "DHS should incorporate terrorism estimates such as these, along with natural disaster risk estimates, into the assessment process to support grant allocations and other assistance to states and localities. Further, DHS should consider investing in the extensions of insurance-industry models noted previously to improve the usefulness of this approach to homeland security analyses."[41] In order to realistically plan for and offer measurable protection against threats, we should apply models that already have identified consequence as a variable equal to threat and vulnerability—the very point of this thesis. If this type of guidance were available to local planners, they would be able to better formulate a risk management strategy.

---

[38] Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, 474.

[39] Bier, *Choosing what to Protect*, 607-620, 611.

[40] U.S. Government Accountability Office, *Homeland Security Grants: Observations on Process DHS used to Allocate Funds to Selected Urban Areas*, 29.

[41] Willis and others, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, Summary, xv.

B. CHALLENGING THE THREAT ASSUMPTION

Since the color-coded threat index was first introduced in March 2002, New York City continues to be at a state of Orange Alert. "The increased emphasis on soft targets seen overseas may be replicated in the United States in large part because more prominent venues have become hardened. Since September 11, concerted moves have been made to upgrade security around high-profile landmarks such as the Pentagon, the White House, the Capitol, state legislature offices, and foreign diplomatic missions. These initiatives have exacerbated the difficulty of attacking prominent sites in the United States. In so doing, this has arguably triggered a process of potential threat displacement toward softer targets such as sports stadiums, shopping malls, hospitals, restaurants, nightclubs, cinema complexes, office buildings, airport arrival halls, and train stations. There are a plethora of these venues across the country, which, given their emphasis on public access, necessarily preclude the type of intrusive and sustained security that can be placed around "high-value" targets. Moreover, because large congregations of people typically gather at these locations, the opportunity for achieving a large number of casualties is significantly increased."[42] Planners must critically evaluate defensive strategies side-by-side with consequence reduction strategies, to determine which approach best meets all their needs, including but not determined by cost savings.

The concept that each region or metropolitan area of the entire nation was under a uniform level of threat was challenged in a 2007 RAND study of the UASI regions. The risk assessment tool mentioned earlier as the Probabilistic Terrorism Model was applied in three ways: 1) evaluate how threat reduces risk, 2) generate terrorism threat profiles for specific cities or regions, and 3) apply threat modeling to guide intelligence analysis. This model used eight target groups such as government buildings, business districts, transportation, industrial

[42] Libicki, Chalk and Sisson, *Exploring Terrorist Targeting* Preferences, 74-76.

facilities, power plants etc. to assess threat. These target groups included a variety of subjective asset characteristics such as high consequence, high value, and high iconic value.[43] The study findings concluded that 95% of the total terrorism risk in the United States is concentrated in eight urban areas: New York City (62%), Chicago (12%), and six other cities (Washington, DC, San Francisco, Los Angeles, Boston, Houston and Philadelphia combine for 21%). The remaining thirty-seven UASI regions shared a cumulative total of 5% of the national risk. If the stated intent of the UASI funding is to "fund high-risk urban areas based on risk and effectiveness,"[44] there is compelling evidence to suggest that the formula for the risk based approach is not effective, reliable or even purposeful in identifying risk. The UASI program is not on a solid strategic footing, and the funding allocations are dispensed according to flawed threat assumptions or simply ignorance to the grant management problems identified in random audits conducted by DHS. The political pressure brought to bear on DHS when the risk based approach was introduced also speaks to the programs' objectivity.

C. RANDOM AUDITS

The Department of Homeland Security Office of the Inspector General audits UASI, HSGP and other first responder grant awards to states on a random basis. Seven audits were done: Colorado, Florida, Pennsylvania, New Jersey, North Carolina, Virginia and Georgia have yet to receive a clean bill of health. Embarrassing as it is, the results were indicative of grant allocations that lacked accountability in the spending process. The audits revealed poor purchasing controls, unauthorized expenditures, late or missing performance reporting and failures to allocate funding to high risk areas or according to state HLS strategies. It is important to note the failures of the following states that were audited:

---

[43] Willis and others, *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*, 9.

[44] U.S. Department of Homeland Security, *FY 2007 Homeland Security Grant Program.*

- The State of Colorado was cited with failing to follow state HLS strategy, grant management lapses, and expenditures that did not comply with grant guidelines and funding allocated to low risk projects. The report goes on to question $12M in costs for both the UASI and HSGP grants between 2003 and 2004.[45]
- Georgia was found to have failed to identify homeland security needs, used a centralized purchasing system that was ineffective, failed to effectively monitor sub-grantee contracts, and failed to allocate funds in a timely manner or properly. The report dismissed the reliability of the state strategy, stating that data in some categories were demonstrably incorrect. The survey reported the number of hazardous material teams to be 92, while only 38 such teams existed. Jurisdictions may have reported on the same threats and vulnerabilities. The survey offered no means of qualitatively assessing actual dangers posed by locally perceived threats and vulnerabilities. The 715 Potential Threat Elements identified statewide were exaggerated and have not yet been validated.[46]
- Florida was cited for ineffective controls to ensure compliance with grant guidelines and sub-grantee contracts.
- Pennsylvania reportedly tracked $150M in UASI and HSGP grants from 2002 through 2004. DHS uncovered $721K in unsupported and undocumented expenditures, late financial and progress reports, failure to monitor performance for effectiveness against strategic goals, and the final expenditure reports and the audits did not agree.
- New Jersey had to return $247K related to unsupported expenditures of the $115M in grant funds received between 2002 and 2004 because adequate documentation did not exist among some sub-grantees.
- Virginia did not allocate funds on basis of risk and did not monitor local government programs adequately. The state purchased $417K in unauthorized equipment out of the $53.5M funds received between 2002 and 2003.

---

[45] U.S. Department of Homeland Security, Office of Inspector General, *Audit of the State of Colorado Homeland Security Grant Program* (Washington, DC: Department of Homeland Security, 2007), https://www.hsdl.org/homesec/docs/dhs/nps36-010308-02.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

[46] U.S. Department of Homeland Security, Office of Inspector General, *The State of Georgia's Management of State Homeland Security Grants Awarded during Fiscal Years 2002 through 2004* (Washington, DC: Department of Homeland Security, 2008), https://www.hsdl.org/homesec/docs/dhs/nps23-021108-02.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008), 12.

- North Carolina – Unreliable accounting for grant expenditures and reduced capability to monitor grants in an adequate fashion were problems brought to light in North Carolina. The Inspector General cited reduced compliance assurance with the Office of Domestic Preparedness program guidance and related regulations, reduced security of sensitive assessment and vulnerability data, lack of consistency, effectiveness, and efficiency in administering grants, and reduced assurance that grant purchases have and will enhance terrorism preparedness and increase interoperability across responder disciplines. All of these findings were results of the audit of the $58M the state received between 2002 and 2003.[47]

The official reports of the problems that states have in securing funds, targeting projects and spending within grant lifetimes reinforce the growing perception that the grant programs were hastily put together to address problems that may not be critical to the high risk threat. News reports frequently turn up stories that highlight failures within the grant process, stories like the purchase of an air-conditioned garbage truck with homeland security grants in Newark, New Jersey, and the purchase riding lawnmowers used for racing in Texas. The publicity enrages taxpayers, embarrasses politicians and delights late night talk show hosts, but it does point to glaring problems in the country's anti-terrorism strategy. With the nation's sense of security shattered by 9/11, it appears that Congress responded by throwing money at both real and imagined problems. Decades of status quo existed within the emergency response discipline, and receiving an influx of money like this was welcomed by first response and public safety agencies. The bottom line is that the similarity of problems uncovered by the DHS audits proves that states and local governments are ill prepared to control the funds or effectively target their use.

This chapter reviewed two grant programs administered by DHS to promote local homeland security. The strategic basis for the UASI and HSGP grant programs has been called into question on two critical issues–-the risk

[47] U.S. Department of Homeland Security, Office of Inspector General, *The State of North Carolina's Management of State Homeland Security Grants Awarded during Fiscal Years 2002 and 2003* (Washington, DC: Department of Homeland Security, 2006), https://www.hsdl.org/homesec/docs/dhs/nps22-112706-03.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008), 2.

based approach itself as well as its effectiveness. First, it was found that not all grant recipients are under high risk as identified in the risk based formula. In fact, most of the risk was centered in eight cities. In addition, the management of the funds at the local level has been questioned in every audit performed by DHS. These facts imply that there is a better use for the limited federal funds. Funding should be targeted at local preparedness building strategies aimed at consequence mitigation.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONSEQUENCE ASSESSMENT

There is currently a failure to understand the complexity of consequences and the dangers of oversimplifying them during planning. Federal guidance on consequence assessment will reveal the ubiquitous federal focus on short term planning. Assessments of consequences, such as the psycho-social issues of mega-catastrophes are avoided during planning stages, allowing planners to dismiss the long term impact of the risk. Many data sources are discussed to assist planners tasked with developing a consequence assessment to begin to enumerate the impact consequence has during the assessment process.

A. FAILURE TO UNDERSTAND

In 2007, The National Infrastructure Protection Plan (NIPP) was announced; Homeland Security Secretary Michael Chertoff is quoted as saying, “the conse2quences of an assault against America's vast network of critical infrastructure sites could be dire, both in loss of life and in economic impact; at the same time, we must avoid imposing onerous security measures that would damage or make economically impractical the very systems that we're trying to protect. The security roadmap announced today reflects unprecedented coordination among the public and private sectors. These plans are already significantly strengthening vital infrastructure and reducing vulnerability to all hazards–terrorist attack and natural disaster alike."[48] It is safe then to refer to consequence as the magnitude and type of damage resulting from successful terrorist attacks and applied to a natural disaster, an industrial accident, an economic downturn or any event that causes harm in some way.[49] However,

[48] Michael Chertoff, "DHS Completes Key Framework for Critical Infrastructure Protection," US Department of Homeland Security, http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm (accessed July 7, 2007).

[49] Willis, *Guiding Resource Allocations Based on Terrorism Risk*, 599.

consequence assessment is yet to be fully employed because the ability to accurately account for consequence is hindered by the complexity of the process and the variety of information sources.

In an unpublished essay, Mr. Robert Ross, a Deputy Director in DHS's Science and Technology Directorate, elaborates on the nature of consequence by illustrating how consequences are comprised of factors that encompass a range of varying scale and dimension.[50] It is the complexity of consequence that defies description. Throwing a pebble into a pond produces a series of concentric ripples. Throwing a hand full of pebbles into a pond produces a pattern of concentric ripples that add and subtract from each other in a confusing configuration of waves. This is the picture of disaster consequences. The interrelationships and interdependencies present a confusing array of information that has to be evaluated and analyzed. Hence, the reality is that the default parameter that defines consequence in any risk reduction method is dollars. Although dollars may be the least common denominator, it neither adequately portrays the human and social costs nor describes the extent or impact of the consequences of a terrorist attack or natural disaster. This one dimensionality discourages development of alternatives to defense based planning. The ability to measure the impact of disaster is something we, as a community, can certainly relate to. For example, the September 11, 2001 attack and Hurricane Katrina have provided us with a much better idea of the breadth and depth of the consequences of major catastrophic events specifically relative to the human, economic and social impacts a disaster can have on the planning, response and recovery stages.

We get hit hard when consequences are felt, seeing how far they reach back and realizing the impact of direct and indirect costs of a disaster. Still, despite this knowledge, there is no empirical method to forecast the consequences of an attack or natural disaster. By quantifying consequences as

[50] Robert G. Ross, "Combating Terrorism with Risk-Based Strategies," (Draft Paper, 2006).

an integral component of a risk assessment, policy makers can visualize the effects of a disaster and determine the best cost-benefit ratio between defense and mitigation. Yet, as long as consequences continue to be viewed as generalized abstractions there will be no incentive to view mitigation as a strategic element of Homeland Security. A hallmark of a catastrophe is in the rapid degeneration of the situation and the cascade of failures that occur. Events unfold in rapid succession, and responders find themselves unable to resolve one problem before a new one evolves. In these situations, responders are steeped in a reactive posture, letting the events form the response. Progress against the incident will not be made until responders transition into a proactive response mode, anticipating problems before they occur, and setting solutions into play before problems get out of control. Assessing the consequences prior to occurrence can forewarn the responder of what to expect and shorten the interval to transition from reactive to proactive response.

A comprehensive consequence assessment can be incorporated into the risk assessment process, but should include specific categories and measures capable of revealing response and resilience factors. State and local planners must be able to quantify needed response resources and resilience building measures. The process then will aid policymakers to formulate a vivid picture of consequences so they can objectively choose between defensive and mitigation options when planning their homeland security strategy. The primary benefit is having a critical review of the range and nature of consequences during strategic policy development, especially when allocating finite resources to homeland security programs. Both human and economic measures of consequence reduction must be incorporated into the risk assessment formula.

B. FEDERAL GUIDANCE ON CONSEQUENCE ASSESSMENT

Local emergency planners are responsible to align their planning and preparedness efforts toward four critical documents as set forth by the Department of Homeland Security. The federal documents include: 1) The

National Infrastructure Protection Plan (NIPP); 2) National Strategy for Homeland Security; 3) National Response Framework, consisting of twenty-two Emergency Support Functions (ESF); and 4) The National Preparedness Guidelines, that includes a planning checklist known as the Universal Task List (UTL) as well as a Target Capabilities List (TCL) which provides a benchmark for assessing preparedness. The purpose of these documents is meant to guide local officials not only in developing their planning and preparedness plans, but also to provide a uniform and consistent baseline methodology among local, state and federal responses to any given event. The main drawback with these documents is that they are all heavily response biased. Recovery issues are strictly short term.

The NIPP, for example, is a guidance document provided to planners to assess all risks in the area of Critical Infrastructure Protection–-the key word here is protection. The NIPP describes certain protective actions to be identified when assessing consequence, vulnerability and threat:

- **Consequences:** Protective programs directly limit or manage consequences by reducing the possible loss resulting from a terrorist attack or other disaster through redundant system design, backup systems, and alternative sources for raw materials or information.
- **Vulnerability:** Protective programs directly reduce vulnerability by decreasing the susceptibility to destruction, incapacitation, or exploitation by correcting flaws or strengthening weaknesses in assets, systems, and networks.
- **Threat:** Protective programs indirectly reduce threat by making assets, systems, or networks less attractive targets to terrorists by lessening vulnerability and lowering consequences. As a result, terrorists are less likely to achieve their objectives and therefore, less likely to focus on the CI/KR (Critical Infrastructure/Key Resource) in question.[51]

Not only are emergency planners utilizing the NIPP guidance document in their planning efforts, but public and private sector entities often include risk management frameworks in their business continuity plans because the planning

[51] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 47.

methodology includes the process of being able to identify assets, assess the risks, prioritize the problems, measure the performance and implement a strategy capable of protecting the program.[52] Businesses are more likely to resort to mitigating solutions to reduce consequences in the form of business interruptions. Local government agencies do not investigate mitigation solutions because of their predisposition to defensive and short term response options. The consequence of an attack or incident continues to be framed in ways that reduce impact to the functionality of the asset rather than impact to the community. Defensive actions, redundant supply chains or systems are all protective strategies. The NIPP is not intended as community protection guidance, yet it does refer to a local role in the protection of assets in their jurisdiction.[53] The NIPP pushes preparedness planners toward defensive and response based planning efforts rather than mitigation or recovery based solutions.

In 2007, The National Strategy for Homeland Security was revised to unify our nation's homeland security efforts by focusing its efforts on four goals: 1) prevent and disrupt terrorist attacks, 2) protect the American people, our critical infrastructure, and key resources; 3) respond to and recover from incidents that do occur; and 4) continue to strengthen the foundation to ensure our long-term success. "While the first three goals help to organize our national efforts, the last goal entails creating and transforming our homeland security principles, systems, structures, and institutions. This includes applying a comprehensive approach to risk management, building a culture of preparedness, developing a comprehensive Homeland Security Management System, improving incident management, better utilizing science and technology, and leveraging all instruments of national power and influence."[54] All aspects of government vital to the

[52] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 105.

[53] Ibid., 23.

[54] U.S. Homeland Security Council, *National Strategy for Homeland Security*, 1.

health, safety and well being of our citizens must be strengthened and officials prepared to lead and sustain the nation during and following a catastrophic emergency.

Revised in January 2008, *The National Response Framework* is the most recent and up–to-date guide to federal response in an all-hazards framework focusing on response and short term recovery. The framework includes fifteen ESFs as "critical mechanism to coordinate functional capabilities and resources provided by Federal departments and agencies, along with certain private-sector and nongovernmental organizations. They represent an effective way to bundle and funnel resources and capabilities to local, tribal, State, and other responders."[55] The application of the framework to local planning, however, lowers the planning horizon to short term objectives and immediate response. The need for detailed consequences is not apparent when the planning horizon is lowered because the catastrophic impacts lie just below the response horizon. If consequences are assessed in detail at this point, the need for a higher level of preparedness becomes apparent, and the planning horizon is raised to study long term recovery needs. So, rather than support the National Strategy for Homeland Security, the National Response Framework can actually diminish the resilience and preparedness of the nation by focusing on the narrow slice of an emergency, identified as the "initial response."

The National Preparedness Guidelines is the Readers Digest Version of seventeen homeland security documents. It inexplicably combines the National Homeland Security Strategy and four other strategies, resulting in a convoluted preparedness master plan that utilizes three planning tools. The first tool is the fifteen National Planning Scenarios that assist local planners to focus government and private sector response resources. Next is the Universal Task List (UTL), a set of sixteen hundred unique tasks, expected to somehow

[55] U.S. Department of Homeland Security, *National Response Framework* (Washington, DC: Department of Homeland Security, 2008), http://www.fema.gov/pdf/emergency/nrf/nrf-base.pdf (accessed March 17, 2008), 57.

"facilitate efforts to prevent, protect against, respond to, and recover from the major events that are represented by the National Planning Scenarios."[56] The downside to the UTL is that although it does address planning and long term recovery issues, in very general terms, missing is a method to assess long term needs so that planners can determine what they are planning for or recovering from. The recovery mission section within the UTL calls for the provision of long and short term medical and mental health services, restoration of the environment and restoration of government and public utility services. Then there is the Target Capabilities List (TCL) in which there are thirty-seven specific capabilities in which every community is expected to plan towards responding to the incident scenarios.

A common task of the TCL is a consequence analysis of critical infrastructure. This consequence analysis should measure the expected outcome of specific scenarios based on analysis of the susceptibility to attack of the asset, given the functional characteristics of the targets, likely cascading impacts to interdependent assets, and the availability of response and recovery capabilities.[57] This is an important concession to consequence assessment. Missing, again, is guidance on the how-to when considering the impact necessary to facilitate preparedness rather than response. The National Planning Scenarios (NPS) provide some of this guidance by detailing information in each scenario that can be applied to any locality by a planner with very little imagination. The NPS encourages consequence assessment at the local level and provides enough information to get the process started. Numerous documents, thousands of pages and mixed messages intimidate planners, forcing them to assert their own approach in assessing risk.

---

[56] U.S. Department of Homeland Security, *National Preparedness Guidelines* (Washington, DC: Department of Homeland Security, 2007), 45. http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf (accessed March 18, 2008), iii.

[57] Ibid., 50.

C. CONSEQUENCE OF MEGA-CATASTROPHES

Hurricane Katrina and September 11th could each be categorized as a mega-catastrophe. The Blue Ribbon Panel on Mega Catastrophes of the Financial Services Roundtable defines a mega-catastrophe as "a natural or man-made event that has *significant* adverse *national* impacts on economic activity, property or human life."[58] Hurricane Katrina made landfall on August 23, 2005, and eighteen months after the catastrophe, on April 19, 2007, Senator Mary L. Landrieu addressed the Senate Subcommittee on Disaster Recovery Hearing and stated that 56,668 residents of Louisiana still lived in temporary FEMA trailers. On July 10, 2007, New Orleans Mayor Ray Nagin reported to the United States Senate Committee on Homeland Security and Governmental Affairs that there were still more than 150,000 residents who remain displaced by the storm. Disasters can last for several days; months, even years, and the impact to a community can last forever in several different ways.

The role of mental health in the response and recovery phases of a disaster changed the view of many especially after 9/11 and Hurricane Katrina. In both events the role of mental health started as supportive but because of the magnitude of these events their role evolved seamlessly into a long-term therapeutic role, eventually being overextended and overwhelmed. The botched response to Hurricane Katrina set the stage for a botched recovery, and the lack of permanent housing appeared to be the key element. Throughout the region there was loss of life, social disruption, property loss, and extensive damages that resulted in numerous adverse effects. A disaster was declared under The Robert T. Stafford Disaster Assistance and Emergency Relief Act, long after the initial event had passed. Extraordinary circumstances forced relief measures to continue and yet even though housing assistance was extended several times,

---

58 Financial Services Roundtable, Accelerating the Katrina Recovery: An Interim Report by the Blue Ribbon Commission on Mega-Catastrophes of the Financial Services Roundtable (Washington, DC: Financial Services Roundtable, 2006), http://www.fsround.org/publications/pdfs/KATRINAFinalDocument.pdf (accessed March 13, 2008), 4.

each deadline that approached caused additional, compounded stress. The perceived insensitivity of the government to the basic sheltering needs of the victim dispels the belief of the victim and the public that there is a caring bureaucracy. Jobs were scarce, lives were disrupted, and relief was nowhere in sight--brutally highlighted as the media coverage to the general public continuously exposed the negligence of federal, state and local response to the situation. The traumatic conditions allowed for a social pathology that created new victims on a daily basis.

The psychosocial consequences of disasters are frequently overlooked in the planning process. However, they appear in the spotlight when an emergency becomes a catastrophe. Mental health concerns are underrepresented in the homeland security disaster planning and preparedness phases because they are primarily recovery functions, and thus invisible to responders. There lacks a connection to or feedback loop incorporating mental health services into the planning process. Once the immediate needs of the first responders are met, mental and public health workers are on their own, because Emergency Operation Centers (EOC) are demobilized and public and mental health workers left to operate within their normal span of resources. Emergency operation plans only address mental health functions that serve the purpose of the first responder. There continues to be limited effort to identify functions necessary to serve the needs of mental health and public health components during the recovery phase. The National Response Framework is expected to be the basis for all local emergency operations plans, and it deals exclusively with short term response and recovery. "**Short-term recovery** is immediate and overlaps with response. It includes actions such as providing essential public health and safety services, restoring interrupted utility and other essential services, reestablishing transportation routes, and providing food and shelter for those displaced by the incident. Although called 'short term,' some of these activities may last for weeks.

Long-term recovery, which is outside the scope of the *Framework*, may involve some of the same actions but may continue for a number of months or years, depending on the severity and extent of the damage sustained."[59]

The lack of medical and public health resources creates a stress on the social fabric of the community particularly in the presence of so many other traumatic conditions. A detailed consequence assessment can work to create the short term and long term connection if experienced mental health and public health leaders are included in the planning phase. We need to realize that disasters cast a wide net--in addition to those directly affected by the disaster, victims can be first responders, witnesses (in person or media exposed), and almost anyone that feels some sort of a connection to the event. The psychological effects of a disaster can have both short and long term effects. Short term--sub clinical--effects can manifest in anxiety, sleep disorders, loss of concentration; these, however, are normal reactions to stress that dissipate in a matter of days or weeks. Longer-term effects do not dissipate but worsen, and are considered abnormal reactions. The unknown impact of post traumatic stress disorder (PTSD) symptoms that occur typically ninety days after an event persist indefinitely, exacerbated by a self medicating increase in drug and alcohol use. Emergency responders are familiar with Critical Incident Stress Management (CISM); assistance is immediate, but short term, much like their operational responses that usually have duration of forty-eight hours. This is similar to the forty-eight hour rule of thumb for catastrophes: you are on your own during the first forty-eight hours. The role of mental health is essentially irrelevant to first responders because the primary mental health role occurs after the initial response, well into the recovery period.

The South Central Center for Public Health Preparedness presented a web cast entitled *Two Years Later: Continued Psychological Difficulties of First Responders and the Affected General Population Post Katrina*, and discussed

[59] U.S. Department of Homeland Security, *National Response Framework,* 45.

the social and mental health conditions that continued to afflict the victims of the hurricane. Symptoms of mental disorders were increasing rather than decreasing. A lack of preparedness is resulting in worsening conditions rather than an improving situation after two years and $85 billions of dollars in disaster relief. Not only does the report identify the glacial pace of the recovery efforts but it points to the fact that prior to the storm the area had the worst economic and health conditions among the general population in the entire country. These facts closely resemble a slow rolling disaster situation rather than a recovery effort. Was this a failure of response, planning or preparedness? Answers to questions like this and lessons learned from disasters are two areas planners can apply in consequence assessments. New Orleans is a perfect example because the probable consequences of a catastrophic hurricane were well known to emergency response planners. If we as first responders fail to apply lessons learned, either from scenario exercises or real time events, the public will lose trust in our ability to provide emergency services and continue to question our practices, procedures and planning efforts.

1. Taking Consequences Seriously

It was July 2004 when the Federal Emergency Management Agency (FEMA) and emergency managers in southeast Louisiana conducted an exercise called Hurricane Pam, designed to assess the consequences of such a storm. This exercise was a departure from the normal plan-exercise cycle, when one develops a plan and designs an exercise to test the plan. Ironically, Hurricane Pam was designed to first identify the consequences of the disaster and then plan to respond to it. In his testimony before the Senate Homeland Security and government affairs Committee, Former FEMA-Louisiana Chief Sean R. Fontenot described his reaction to the exercise this way: “usually, you write a plan and then have an exercise. However, when it was explained to me that we were going to take an exercise scenario which generated real consequences and real data and bring operational level people in so they could make decisions using the

real data and consequences which could then drive the writing of a plan, I quickly got on board. I championed the fact that we were using operational people to write this plan because there are too many times plans are written without taking the operational aspects into account and this leads to non-usable plans."[60] The Hurricane Pam exercise was a logical departure from the usual plan-exercise cycle, except it yielded extremely accurate consequence projections.

The design consultant for the exercise said, "We wanted to create a sense of realism in the exercise which generally does not inform a planning process when you are dealing with emergency planning. Because we are all mortal beings, we don't like to look at the face of death and disaster, and most planning tends to look at the event that you can manage, not the events that you can't manage. The Hurricane Pam exercise was designed with detailed consequences down to the parish level for each of these data elements. We actually had data on how many people would be affected by parish so that each of the individual parishes and the State and FEMA would have tactile information at their fingertips that they could use in planning."[61] Once the public became aware of this fact, fingers were pointing and the "being so surprised" attitude to this disaster was insulting to the residents of Louisiana. This is exactly the reason that when agencies exercise their plans it is critical to fix the issues revealed so that, at the very least, it can't or won't happen again. One can't say that we didn't know!

Consequence assessment should be taken seriously; the public health sector knows this first hand while planning and preparing for a possible influenza pandemic. An example of planning by current methods might begin by expecting that during a pandemic of a highly pathogenic influenza, as many as one third of the residents of Union County, New Jersey will require medical care, which will

---

[60] U.S. Senate. Committee on Homeland Security and Governmental Affairs, *Preparing for a Catastrophe: The Hurricane Pam Exercise* (Washington, DC: Government Printing Office, 2006), https://www.hsdl.org/homesec/docs/legis/nps20-011007-06.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008), 11.

[61] Ibid., 18.

seriously overwhelm hospital surge capacity. This is qualitatively different from saying 130,000 people will need medical care even though we know there are less than 1600 hospital beds available at full surge capacity. The first statement is vague enough to allow a planner to consider that the problem will have a resolution. The second statement allows no such delusion. Another example is to say that an anthrax attack against Atlantic City, New Jersey will result in great loss of life and serious economic costs in the first seven days. This statement is not as instructive to HLS planners as saying that 33,000 people will die and another 22,000 will require medical care costing $326.7 million, there will be 210,675 years of potential life lost, over $26.2 billion actuarial losses, 50,000 jobs lost, $734,000 loss of state and federal income tax losses, $874,000 in other lost tax revenues and a loss of $4,380,000 per day in sales of goods and services to the casino industry.[62] When the simple consequence statement is replaced with a quantitative statement of the losses, the practicality of mitigation and preparedness is difficult to miss. It is important to note that there are few defensive options available to local planners to either of the above examples, but the preparedness and mitigation efforts for both scenarios are nearly identical. In these two cases, preparedness and mitigation efforts would have dual-use functionality as well as day-to-day utility.[63] This is an advantage that a comprehensive consequence assessment can provide planners; it can suggest mitigation measures that will reduce consequences and build resilience while reducing risk.

D. ELEMENTS OF CONSEQUENCE

September 11, 2001 and Hurricane Katrina were incidents that taught us many things about consequences and the difficult road to recovery. Despite the

---

[62] Richard B. Proctor, "Assessing the Impact of a Successful Biological Weapons Attack," *New Jersey Municipalities Magazine* 78, no. 2 (2001), 6-10.

[63] Denise Santiago and Anka Richter, "Assessment of Public Health Infrastructure to Determine Public Health Preparedness," *Homeland Security Affairs* 2, no. 3 (2006), 1-25, http://www.hsaj.org/pages/volume2/issue3/pdfs/2.3.11.pdf (accessed August 27, 2007).

relatively small geographic footprint of the World Trade Center attack, there was approximately $94 billion in estimated loss with economic ripples felt well beyond New York City.[64] Katrina, on the other hand, devastated an area roughly the size of Great Britain, and after more than two years, and despite more than $30 billion in federal relief, significant problems still exist in areas like New Orleans and Gulfport-Biloxi.[65] Studies on the aftermath of Katrina and the 9/11 attacks reveal many sources of information quantifying consequences that were previously overlooked. Impacts of Katrina to housing, industrial output, employment, travel and tourism, energy, import-export, gaming, fisheries and federal aid are well documented from data collected routinely by the federal government. If these elements were incorporated into the risk assessment process we would have a much clearer idea about the real cost of consequences and what vulnerability reduction measures cost in terms of lost opportunity to reduce consequences.

The Census Bureau website[66] is an important source of critical information including individual and family income, housing descriptions and median values as well as employment status. The Census Bureau also has economic and business data broken out by zip code for eight business sectors, which encompass about 60% of the businesses that have employees. The American Fact Finder feature can sort out business information by annual net proceeds so that the impact of a business disruption can be estimated. Census Bureau County Business Patterns provides data on establishments that include employment numbers, first quarter and annual payrolls. This can help planners predict the volume of unemployment claims due to employer closures, or loss of business due to travel restrictions, illness, etc. The U.S. Commerce Department, Bureau of Economic Analysis has regional economic information that includes

[64] Economics and Statistics Administration, *The Gulf Coast: Economic Recovery Two Years after the Hurricanes* (Washington, DC: U.S. Department of Commerce, December 2007), https://www.esa.doc.gov/Reports/2008/GulfCoast2yrdec2007.pdf (accessed March 17, 2008).

[65] William P. Thompson Jr., *One Year Later: The Fiscal Impact of 9/11 on New York* City, 3.

[66] U.S. Census Bureau, Census Bureau Economic Programs, Business and Industry webpage, http://www.census.gov/econ/www/index.html (accessed March 9, 2008).

income by county, unemployment, dividends, etc.[67] The Bureau of Labor Statistics has a wide array of data on all aspects of employment broken out geographically and by North American Industry Classification System identification number.

A study conducted one year after 9/11 by the Comptroller of New York City showed the value of locally collected data. The report examines six (6) categories of economic factors that adversely impacted the City. These include:

- Lost wealth – property and human potential
- Lost gross city product including lost jobs
- Tax revenue lost
- Increased expenditures
- Unexpected capital costs
- Impact of federal assistance[68]

The report also projects anticipated future losses based on economic growth prior to the attack, the immediate losses experienced in the attack, and the projected economic rebound after the attack. This report shows how much can be brought into the consequence assessment process if the planner takes the time to build out the scenario.

Congress established the September 11th Victim Compensation Fund (VCF), after the 9/11/ attacks to compensate those who were seriously injured or killed in the attack. The VCF is a unique loss category of the 9/11 attacks, but it is one that will arise in future terrorist attacks and must be considered in future consequence assessments. Although individual cases are not open to the public, we know that:

> Almost all civilians who were killed or seriously injured in the 9/11 attacks decided to file claims with the VCF. Awards from the VCF ranged from $250,000 to $7.1 million and averaged $2.08 million.

[67] U.S. Department of Commerce, Bureau of Economic Analysis, Regional Economic Accounts webpage, http://www.bea.gov/regional/index.htm (accessed March 9, 2008).

[68] Ibid.

> Quantified benefits for the 2,551 killed and 215 seriously injured totaled $8.7 billion, or an average of $3.1 million per recipient, with 69 percent of total benefits coming from the VCF, 23 percent from insurance, and 8 percent from charity.[69]

With payouts to family members of victims averaging $2.08 million dollars, the cost of successful future terrorist attacks has increased significantly.[70] Cost is the universal parameter for loss, and planners must account for as many costs as possible while conducting a consequence assessment.

The planner must ask questions concerning the geographical footprint of the incident. Within that footprint he/she will need to know the population characteristics; number of people in the area; if that population changes significantly by time of day; loss of income impact; and type of businesses. Who will be impacted by the loss of product? How much time to return to normalcy? What is the impact to the local economy and the regional economy of the disruption? Other criteria's in a consequence assessment include real estate uses (residential, industrial, commercial); the nature of public property (are response assets located within the footprint, delaying response, i.e., hospitals, fire stations, EMS units?). What is the value or replacement cost of property impacted by the incident?

Casualty estimates are another area that planners have to address. The Centers for Disease Control have several sites that can assist planners to estimate the numbers and type of casualties to expect from an incident. The Mass Casualty Predictor[71] provides information useful to estimate hospital utilization. From this site there are links to more specific pages that list common bacteriological and chemical agents, their effects and common medical management recommendations, as well as a mental health estimator. There are

---

[69] Lloyd Dixon and Rachel Kaganoff Stern, *Compensation for Losses from the 9/11 Attacks* (Santa Monica, CA: RAND Corporation, 2004), 7-9.

[70] Ibid., 8.

[71] Centers for Disease Control, Mass Casualties Predictor webpage, http://www.bt.cdc.gov/masscasualties/predictor.asp (accessed March 17, 2008.).

also links to pages that contain radiological exposure and treatment information as well as pages that give background information on blast injuries and treatments based on actual terrorist incidents. Types of injuries and medical management recommendations can serve as the basis for cost of treatment projections for the estimated casualties. Medicare, Medicaid and private medical insurers all have Usual and Customary Rates (UCR) and Allowable Charge figures for various treatments. Mining the data from known disasters and pairing them with cost of treatment estimates can give cost of treatment averages for various types of injuries or estimates can be attempted from recommendations for medical management paired to UCR's from regional health insurers. These costs have to be considered when policy makers are deciding where to invest Homeland Security funds. The more accurate the consequence assessment becomes the better policymakers can determine the cost effectiveness of security measures.

This chapter illustrated the importance of understanding the complexity of consequences. It revealed how relevant federal guidance documents focus on short term, response oriented issues, lowering the planning horizon and thus limiting our ability to improve response to incidents to only incremental improvements. This shortcoming is very evident looking at the medical and mental health recovery from Hurricane Katrina. After two years and billions of dollars the psychosocial fabric of the Gulf Coast community is still tearing. This demonstrates that incremental improvements are ineffective when emergencies become catastrophes. We need resources in scale with the problems they trigger. When we are caught unprepared, local government specifically and all levels of government generally, lose the confidence of the public.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CULTURE OF PREPAREDNESS

In this chapter Post 9/11 responders are discussed in relation to the various new disciplines that are involved in emergency response and in the complexity of today's responses. As the new and traditional disciplines develop stronger relationships there will be a foundation for a true culture of preparedness. The Black Swan phenomenon reveals that despite federal guidance for critical infrastructure protection, it is impossible to predict low probability, high consequence incidents, but it is not impossible to predict their effects. By utilizing consequence assessment we can begin to prepare for the next Black Swan. In building resilience, the importance of the all-hazards approach to preparedness is discussed and how the trust of the public relies on a prepared government.

A. POST 911 RESPONDER

Preparedness is "the range of deliberate critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required activities and resources to mitigate risk."[72] And although these principles have been used to justify defensive and response based options, they are clearly meant to stimulate alternative strategies to the familiar "guns, gates and gadgets" approach. Observing the response to Hurricane Katrina on the Fox and CNN news outlets brought to mind the question, "How could a news crew gain access to the city of New Orleans when emergency responders could not?" The main lesson learned is the need to develop and foster a transformation to a "culture of preparedness."

[72] U.S. Department of Homeland Security, *National Infrastructure Protection Plan,* 104.

There continues to be an overwhelming "it can't or won't happen here" attitude among local emergency management and/or or local policy makers. This is supported by the Nationwide Plan Review Phase II Report which stated that "twenty-one percent of State plans and 9% of urban area plans were rated as Sufficient in terms of feasibility; this corresponds to a prevailing belief discounting the likelihood of catastrophes."[73] The post 9/11 responder has to recognize the probability of an incident of national significance will happen again. There is no part of the country immune from a devastating natural disaster. "While Hurricane Katrina was devastating, catastrophe modelers have identified a number of possible natural disasters that could be much worse. Among these extreme events would be a repeat of the 1906 San Francisco earthquake with potential damages estimates reaching $400 billion; a repeat of the 1900 Galveston hurricane with $36 billion in possible damages; a repeat of the 1938 Category 3 hurricane that hit the Northeast with possible damages exceeding $300 billion; or, a repeat of the series of earthquakes that struck the New Madrid Fault in 1811 and 1812 with potential economic damages of up to $275 billion with insured losses reaching $100 billion. All of these and many more scenarios are possible. Should any one of them occur, we are unprepared to deal with the aftermath of an event of this magnitude."[74] Post 9/11 responders must prepare for highly complex response scenarios by collaborating with other disciplines and the public and the private sector.

Within the emergency management culture are long standing biases toward response rather than mitigation, which was clearly illustrated in the NRF's distinction between short term response and long term recovery. This collective denial inhibits any transformation to a culture of preparedness and promotes a conflation of preparedness and readiness. Responders need to know how and where to go for additional resources once they hit their breaking point. Without an

---

[73] Nationwide Plan Review Phase II, 62. *Nationwide Plan Review: Phase 2 Report*, US Dept of Homeland Security, June 2006.

[74] National Association of Insurance Commissioners, *Natural Catastrophe Risk: Creating a Comprehensive National Plan*, NAIC, (draft document, 2007), 1.

awareness of the probable consequences of an incident they can neither accurately gauge level of preparedness nor identify resources necessary to mitigate the impact. Critical to every response is the interval of time between being reactive and becoming proactive. It is in this transition phase that responders have the ability to keep an emergency from becoming a disaster. The faster responders become proactive the closer they are to entering the recovery phase. Aware that human vulnerability exacerbated by the lack of planning or lack of appropriate emergency management can lead to financial, structural, and human losses, it is critical for responders to respond proactively before the damage of events spirals out of control.

Prior to September 11, 2001, there was a “response as usual” attitude among first responders, and on that very day the lack of a culture of preparedness among emergency responders was highlighted and has affected the way first responders plan, prepare and respond to any disaster today. Most local emergency management organizations were traditionally under funded and/or suffering from dual use positions. For example, “two decades of taxpayer rebellion have stripped away the means necessary for government workers to provide help during emergencies. Most city and state public health and emergency-management departments are not funded adequately enough for them to carry out even their routine work.”[75] Another example is that it was not uncommon for the police or fire chief to also act as the emergency management director. The response to Hurricane Floyd in 1999 raised serious questions about North Carolina’s preparedness and ability to deal with large-scale disasters due to the slowness of the emergency response, the heavy loss of life and the inability to conduct pre-planning. “Local emergency operation centers (EOC) [that] were always used to dealing serially with small-scale incidents like car wrecks and lost person searches were unable to handle a large number of

[75] Stephen E. Flynn, "America the Resilient: Defying Terrorism and Mitigating Natural Disasters," *Foreign Affairs* 87, no. 2 (March/April, 2008), 2-8, http://opim.wharton.upenn.edu/risk/library/J2008Foreign_Affairs_Flynn.pdf (accessed March 13, 2008).

simultaneous incidents. Managers had no training in dealing with floods or large-scale incidents, and the state, which could have provided the needed expertise, adopted a passive, hands off attitude as they attempted to solve each problem as it came up."[76] Response was business as usual in that emergency management directed operations, police directed traffic, firefighters and public works pulled individuals out of the water, and public health officials focused on environmental health and surveillance of disease/injury.

National Strategy for Homeland Security identified that the culture of preparedness relies on four principles. "The first principle of our Culture of Preparedness is a shared acknowledgement that creating a prepared Nation will be an enduring challenge."[77] The second principle is the importance of individual and collective initiative to counter fundamental biases toward reactive responses and approaches. Our culture, therefore, must encourage and reward innovation and new ways of thinking as well as better align authority and responsibility so that those who are responsible for a mission or task have the authority to act.[78] The third principle is that individual citizens, communities, the private sector, and non-profit organizations each perform a central role in homeland security.[79] The fourth principle of our Culture of Preparedness is the responsibility of each level of government in fostering a prepared Nation.[80] Developing a culture of preparedness is very different from preventive and defensive strategies; they are true preparedness and mitigation based approaches to catastrophic problems. They concern the government's ability to provide essential services in emergency conditions and measures to minimize impacts of any major incident that occurs.

Today's responders have a whole new set of priorities, with different professional cultures being thrown into the mix, such as public health and health

---

[76] CFS Press, http://www.cfspress.com/overwhelmedbyfloyd.htm (accessed March 17, 2008).

[77] *National Strategy*, 41.

[78] Ibid.

[79] Ibid., 42.

care agencies. The main challenge is that these public health agencies are more planning oriented by comparison, hopelessly understaffed, have a completely different set of response priorities, and have rarely ever trained with other responders such as emergency management, police and fire officials. Due to the required interaction of unfamiliar agencies and disciplines, it is clear that responses have become much more complex, necessitating the development of plans such as the National Response Framework and the National Incident Management System (NIMS). Emergency response now looks more like a modern military Distributed Operations model than the antiquated phalanx formation.

Moving closer to a cultural change within emergency management will require a paradigm shift that casts all players, new and traditional responders, into the same mix. Preparedness must emphasize the shared nature of responsibilities in a catastrophic event. The shared nature of responsibilities requires us to "develop a shared vision of our commitment to preparedness: what we must do to prevent, protect against, respond to, and recover from the next catastrophe."[81] A new trust has to be established among people and agencies that have little or no experience working together. Cultural institutions and artifacts have to be broken down and reformed. This approach will require that players recognize the shared nature of responsibility in planning and response. Comprehensive consequence assessments can provide a means to visualize a disaster and illustrate the shared relationships and responsibilities. Exercises are another way to accomplish this transformation. Plan revisions after exercises can help to align plans to human and physical assets; align authority to responsibilities; align expectations to capabilities; and, integrate and synchronize our policies, strategies and plans. If this is to be successful, however, it is necessary for policy makers to clearly separate plan failure from individual or

[80] *National Strategy*, 42.

[81] Office of the President, *The Federal Response to Katrina: Lessons Learned* (Washington, D.C.: United States of America, 2006), 66.

agency failure. Removal of blame removes the pressure of failure, creating an environment that encourages innovation and is conducive to improvement.

Instead of defining failure as an unsuccessful attempt at doing something, it should be redefined as inaction or resistance to change within agencies unwilling to plan, trust, reform and exercise as a unit. A culture of preparedness will incorporate a shared vision of readiness, cooperation, capability, innovation and trust. These cultural shifts defy analytical enumeration but can be used as indicators to know whether we are achieving success by observation of increased cooperation, decreased competition and increased communication (formal and informal) among response agencies and personnel. These informal indices are the necessary precursors to build in collaborative capacity.

B. BLACK SWAN PHENOMENON

Nassim Nicholas Taleb, author of *The Black Swan*, writes about how we process information, avoid risks, and fall into traps based on false assumptions concerning probability and possibility. His concepts have application to homeland security in that he argues that it is futile to use a risk based approach to predict something that is unforeseen. He says that "we can have a clear idea of the consequences of an event even if we do not know how likely it is to occur. I don't know the odds of an earthquake, but I can imagine how San Francisco might be affected by one. This idea that in order to make a decision you need to focus on the consequences (which you can know) rather than the probability (which you can't know) is the central idea of uncertainty."[82] The events of 9/11, Hurricane Katrina and the recent sub-prime mortgage collapse are all examples of black swans. The theory is that a black swan possesses three attributes. First, it is an outlier in that it lies outside the realm of regular expectations because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Finally, in spite of its outlier status, human nature makes us concoct

[82] Nassim Taleb, *The Black Swan: The Impact of the Highly Improbable*, (New York, NY: Random House, 2007), 211.

explanations for its occurrence after the fact, making it explainable and predictable. A black swan is the triplet of being a rarity, having extreme impact, and retrospectively predictable.[83]

Black swans are the high consequence/low probability events that are feared by preparedness planners. It was not until after the attacks on the World Trade Center and the Pentagon that the signs and signals observed prior to the attack made sense and eventually led the 9/11 Commission to lament the "failure of imagination" and the "failure to connect the dots." The devastation of the broken levees, the botched response and the equally botched recovery in Hurricane Katrina are examples of events that were completely unexpected in the richest, most powerful nation in the world. It is interesting that in an industry that relies so heavily on risk and probability models to minimize loss that the collapse of the sub-prime mortgage market and the cascade effect on the world economy was completely unexpected by everyone except Taleb. The point is--Black Swans are mega-catastrophes and they are occurring with greater frequency. The problem is–-planning, responding, and dealing with it!

C. BUILDING RESILIENCE

Resilience has become the buzz word of choice in homeland security circles. Resilience broadly defined is the ability of a system to withstand and recover from adversity.[84] Emergency response is the ability to react to an incident, protect life and property to the greatest extent possible, stabilize the situation and pave the way for the recovery effort. September 11, 2001 and Hurricane Katrina were incidents that taught us many things about consequences and the difficult road to recovery. Resilience refers to the ability of a system to absorb a shock without interruption or to bounce back quickly from a potentially fatal blow. Stephen Flynn ascribes four attributes to resilience that describe how

[83] Taleb, *The Black Swan: The Impact of the Highly Improbable*, 8.

[84] Christine Pommerening, Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience (Fairfax, VA: George Mason University, 2007), 10.

resilience affects a system. He writes: First, there is robustness - the ability to keep operating or to stay standing in the face of disaster.[85] Second is resourcefulness, which involves skillfully managing a disaster once it unfolds.

The third element of resilience is rapid recovery, which is the capacity to get things back to normal as quickly as possible after a disaster. Carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are crucial. Finally, resilience means having the means to absorb the new lessons that can be drawn from a catastrophe.[86] These attributes can only be achieved if planners are aware of what is likely to occur in an incident, and how adverse events can be avoided. In short, they need to have thought through the possible consequences; identified key resources; informed all key players; and, have built in redundancies or sufficient reserve capacity to maintain critical functions.

It is important for communities to build their preparedness level because of the nature of recent and most likely future disasters. “The United States is becoming a brittle nation. An increasingly urbanized and suburbanized population has embraced just-in-time lifestyles tethered to ATM machines and 24-hour stores that provide instant access to cash, food, and gas. When the power goes out and these modern conveniences fail, Americans are incapacitated.”[87] We know that our power grid has inherent weaknesses. We know that we are highly dependent on foreign energy sources imported from countries that are less than strong allies. Our “just in time” supply chain has depleted our reserve capacity in every area. We are vulnerable to more and various interruptions and failures than ever before. Resiliency needs to be built

[85] Stephen Flynn, “America the Resilient: Defying Terrorism and Mitigating Natural Disasters,” *Foreign Affairs* 87 no. 2, 2.

[86] Ibid., 3.

[87] Ibid., 1.

on a personal, community and regional basis. Well synthesized by The United States Fire Administration are three characteristics of a resilient community and are as follows:

- Identify and comprehend the multiple vulnerabilities to all hazards resulting from the interdependencies among the departments, agencies, corporations, industries, and organizations that comprise the public and private sectors of a community.
- Meticulously assess the probable consequences of all hazards considering the identified vulnerabilities and the cascading effects of a disaster among all community service providers.
- Develop a community security plan that eliminates vulnerabilities and mitigates predicted consequences to ensure stakeholder functions can be quickly restored after an incident and the community can return to normal operations as soon as possible.[88]

The key to building a resilient community is the ability to comprehend the risks facing it. Comprehension denotes a keen understanding of the risk that includes knowledge of the weaknesses inherent in the infrastructures and how they are vulnerable to various hazards. Comprehension of the risk facilitates the development of continuity plans that in turn rely on regional, interdisciplinary planning and protective measures that include defensive measures, redundancy and mitigation measures. When discussing the long term social and psychological effects of Hurricane Katrina, Dr. C.J. Davis, State Planner from The Mississippi Office of Emergency Planning and Response and the Mental Health Liaison to the Mississippi Department of Health, enumerated the crime, drug abuse, mental health challenges, and pathology found in temporary housing trailer compounds two years after the hurricane and said, “We didn’t visualize this.”[89]

---

[88] "Infogram 18-07: Characteristics of a Resilient Community," U.S. Fire Administration, http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/infograms/ig2007/18-07.shtm (accessed January 31, 2008).

[89] Alabama Department of Public Health, *Two Years Later: Continued Psychological Difficulties of First Responders and the Affected General Population Post Katrina*, November 30, 2007), http://www.adph.org/ALPHTN/default.asp?TemplateNbr=3&DeptID=143&TemplateId=4895 (accessed March 16, 2008).

Achieving resilience is a goal that requires a comprehensive, all-hazards, cross-sector, grass roots-to-national level integrated approach. Resilience requires both horizontal and vertical cooperation and coordination of key public, private, and non-profit stakeholders that have responsibilities or vested interests in improving regional preparedness.[90] A thorough and comprehensive consequence assessment will enhance these resilience building measures and facilitate comprehension. Illuminating the chain of events that are likely to occur and revealing the interdependencies among response disciplines will facilitate cross jurisdictional horizontal and vertical integration. We can't forget that response and recovery will ultimately depend upon a foundation of trust in government. The ability to re-establish a sense of normalcy depends on a trust factor among communities, responders and political governments. It is the speed with which we return to normal that measures our resilience. A prime example of speedy recovery is the aftermath of the World Trade Center attacks. Even though the destruction was a national trauma, New York City returned relatively quickly to normalcy because the City of New York maintained a high level of preparedness. The people of New York refused to give in to the situation because Mayor Giuliani—known as "America's mayor" because of his leadership--showed the same emotions as those hit hard, and in return, he was trusted and praised for his close involvement with the rescue and recovery efforts.

In light of the increasing complexity of today's emergency responses, planning is critical today. Both traditional and non-traditional responders must work together to develop a culture of preparedness. The higher level of preparedness is particularly important to respond to the Black Swan events. Hurricane Katrina and 9/11 can certainly be categorized as black swans because they were unpredictable with high impact.

---

[90] Paula L. Scalingi, "Moving beyond Critical Infrastructure to Disaster Resilience," In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience* (Arlington, VA: George Mason University, School of Law, 2007), 49-72, http://cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf (accessed March 17, 2008), 51.

VI. CONCLUSION

The argument of this thesis has been that the current risk assessment method discourages local governments from carefully considering consequence as an equal part of the risk based equation in protecting their hometowns. Local emergency managers are concerned with ground level issues. They see the consequences of incidents in human terms. Yet they are forced to mold their efforts to conform to federal guidance that is really geared to the 30,000-foot view. Until a thorough understanding of the consequences of an incident is considered and the funding allocation formula revised, local homeland security preparedness efforts will be incomplete at best.

There is limited funding available to local government to defend an unlimited number of targets by applying a risk-based approach that favors defensive tactics over mitigation. Making incremental improvements to respond to or defend against the potentially catastrophic threat is not good enough anymore. There needs to be a consistent method for assessing risk at the local level—one that lessens the impact of the attack or disaster by equally considering threat, vulnerability, and consequence during the assessment process.

Consequences are in fact a complex series of events that are difficult, but not impossible, to envision if the potential incident is carefully thought out during planning. Ironically, Hurricane Katrina provides a perfect example of planning for the worst consequences. New Orleans' exercise in 2004, known as Hurricane Pam, identified many of the needs and lessons to reduce the eventual impact of a real catastrophe. Unfortunately, agencies and leaders failed to implement many of the lessons. By performing a comprehensive consequence assessment we can raise our planning horizon, tell the story of the disaster in a safe environment, identify the necessary resources to reduce an impact, and build the interdisciplinary and interagency relationships required in forming a culture of

preparedness. Should we opt out of taking time to assess consequences during the planning process, Fox News and CNN will be sure to show them to us and to the rest of the world during and after an incident.

Since the inception of the Department of Homeland Security in 2002, billions of dollars have been invested in projects with little relation to national security. The RAND Center for Terrorism Risk Management Policy has found that 95% of terrorism risk is concentrated in eight urban areas. The funding strategy is based on marginal improvement of response capability and defensive measures for targets under no threat. This undermines our ability to build the capacity that we need to reduce the number of victims of the next disaster that we know will come. In addition to the strategic shortcomings of our homeland security grant programs, every random audit of state grant performance uncovered problems stemming from faulty management, dubious targeting of expenditures and/or questionable spending problems.

Disaster planning can also benefit greatly from a comprehensive consequence assessment. The consequence assessment can paint a picture that informs responders and agencies involved in recovery of what to expect, and guide preparedness planning in measures aimed at reducing loss of lives and property. This effort is thwarted, however, by DHS guidance that focuses on short term or defensive options rather than on mitigation plans capable of lessening the impact of an incident. The National Response Framework, for example, is intended for short term planning purposes, or as the title indicates, a *response* framework. The National Infrastructure Protection Plan (NIPP) focuses on defensive options for critical infrastructure/key resources (CI/KR). The key word here is *protection*.

The National Preparedness Guidelines, on the other hand, professes to address both long and short-term preparedness by including a list of Target Capabilities and utilizing a set of Universal Tasks everyone is expected to apply in the planning process. Instead of encouraging a comprehensive planning process, these documents are overwhelming and confusing to a planner. Then

there is the National Strategy for Homeland Security that sets out a plan to prevent and disrupt terrorist attacks, to protect people and CI/KR, and to respond and recover from incidents. The Strategy admits that recovery is an enormous task but one that can be ameliorated by preparedness and developing a new culture of preparedness.

The national strategy lists four elements of the culture of preparedness. Three of the elements in the strategy are assigned to individuals and the private sector. The fourth charges all levels of government to embrace in partnership.[91] There is a subtle but important difference in the description of the culture of preparedness between the National Strategy and *The Federal Response to Hurricane Katrina: Lessons Learned*. The Katrina report identified the high priority of this critical need, stating that "a new preparedness culture must emphasize that the entire Nation—Federal, State, and local governments; the private sector; communities; and individual citizens—shares common goals and responsibilities for homeland security. In other words, our homeland security is built upon a foundation of partnership."[92] Here the leadership role of the federal government is evident in fostering the partnership. Disaster planning, led by a comprehensive consequence assessment, can provide the link between cause and effect, and between the public and private resources required by the culture of preparedness.

Developing a culture of preparedness must begin with the first responder communities as they begin to develop, trust and nurture new relationships within and among dissimilar agencies under the common cause of saving lives. New trust has to be established as unfamiliar partners begin to rely on each other to accomplish their mission. The more new partners participate in assessing consequences the easier it will be to recognize the inter-relationships and inter-dependencies that will either make or break the recovery from a disaster.

---

[91] *National Strategy,* 42.

[92] *Katrina: Lessons Learned*, 79.

A. RECOMMENDATIONS

Since September 11, 2001 this country has spent, on average, $282 millions per day on the "Global War on Terror."[93] Most of the expenditure has been on the war in Iraq. We need to take a few days off from war and concentrate on the home front by increasing our resilience. The resilience of this nation is dependent upon the strength found in each of us as citizens and the preparedness of our governments.

DHS must direct as much attention on preparedness issues as it has on response and vulnerability reduction. Strong guidance on consequence assessment will aid local governments in developing the local resources necessary to build preparedness. Our present strategy relies on multi-hazard reduction instead of all-hazard preparedness. We can no longer depend on the leadership of September 10th to protect us in the future. We need to upgrade the local emergency management leadership to match the increasing complexity that true preparedness requires. Local emergency management directors should be full time federally funded employees assigned to a local jurisdiction. Critical Infrastructure Protection should be focused on sector wide faults and be the responsibility of the federal government. Local efforts should be focused on preparedness, specifically fostering the culture of preparedness and building resilience.

B. COMMENTARY

It is time to end reliance on expensive outside contractors with limited or no local situational knowledge or experience needed to augment local preparedness. Many disciplines suffer from manpower shortages; these areas will require substantial, long term federal funding to expand and maintain the total workforce. Better training of the existing workforce is not the panacea for

[93] Amy Belasco, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*, Report prepared for U.S. Congress, (Washington, D.C.: Congressional Research Service, updated February 22, 2008).

disciplines like public health and mental health. A ten percent increase in productivity in a field that needs to double its workforce just to meet routine operations is an incremental improvement that is insignificant in every condition. DHS has not asked its original workforce to do the expanded roles it has acquired. When intelligence needed to be analyzed, analysts were hired. When airports needed security, new security was hired. As the border needs patrolling, new officers are being hired. State and local governments do not have the ability to hire new staff for HLS roles. This is a serious handicap that must be addressed. Brand new equipment in the hands of the same old short staff will not improve response capability. There is a wealth of knowledge, dedication and resourcefulness resident in local agencies that need only the time and support to perform the critical tasks that lie ahead. We need to scale the workforce to the new role. The belief that incremental improvements to response will somehow reduce consequences more than just incrementally is madness not worthy of the American people.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alabama Department of Public Health. *Two Years Later: Continued Psychological Difficulties of First Responders and the Affected General Population Post Katrina*. Webcast. November 30, 2007, http://www.adph.org/ALPHTN/default.asp?TemplateNbr=3&DeptID=143&TemplateId=4895 (accessed March 16, 2008).

Bier, Vicki M. "Choosing what to Protect." *Risk Analysis* 27, no. 3 (June 2007): 607-620.

Chertoff, Michael. "Testimony of Secretary Michael Chertoff U.S. Department of Homeland Security before the Senate Committee on Homeland Security and Government Affairs." Department of Homeland Security. http://www.dhs.gov/xnews/testimony/testimony_1158336548990.shtm (accessed August 29, 2007).

———. "DHS Completes Key Framework for Critical Infrastructure Protection." US Department of Homeland Security. http://www.dhs.gov/xnews/releases/pr_1179773665704.shtm (accessed July 7, 2007).

Dixon, Lloyd and Rachel Kaganoff Stern. *Compensation for Losses from the 9/11 Attacks*. Santa Monica, CA: RAND Corporation, 2004, http://www.rand.org/pubs/monographs/2004/RAND_MG264.pdf (accessed August 29, 2007).

Economics and Statistics Administration. *The Gulf Coast: Economic Recovery Two Years After the Hurricanes*. Washington, DC: U.S. Department of Commerce, December 2007, https://www.esa.doc.gov/Reports/2008/GulfCoast2yrdec2007.pdf (accessed March 17, 2008).

Financial Services Roundtable. *Accelerating the Katrina Recovery: An Interim Report by the Blue Ribbon Commission on Mega-Catastrophes of the Financial Services Roundtable*. Washington, DC: Financial Services Roundtable, 2006, http://www.fsround.org/publications/pdfs/KATRINAFinalDocument.pdf (accessed March 13, 2008).

Flynn, Stephen E. "America the Resilient: Defying Terrorism and Mitigating Natural Disasters." *Foreign Affairs* 87, no. 2 (March/April 2008): 2-8, http://opim.wharton.upenn.edu/risk/library/J2008Foreign_Affairs_Flynn.pdf (accessed March 13, 2008).

Hartwig, Robert P. "The Cost of Terrorism: How Much cCan We Afford?" Philadelphia, PA, National Association of Business, Economics, 46th Annual Meeting, October 4, 2004. .http://server.iii.org/yy_obj_data/binary/736851_1_0/tria.ppt (accessed August 29, 2007).

"HAZUS-MH Overview." FEMA. http://www.fema.gov/plan/prevent/hazus/hz_overview.shtm (accessed March 17, 2008).

"Infogram 18-07: Characteristics of a Resilient Community." U.S. Fire Administration. http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/infograms/ig2007/18-07.shtm (accessed January 31, 2008).

Lewis, Christopher M. *Terrorism Threats and the Insurance Market*. Testimony before the Subcommittee on Oversight and Investigations of the House Financial Services Committee; and the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the House Homeland Security Committee. July 25, 2006, https://www.hsdl.org/homesec/docs/testimony/nps30-112806-05.pdf&code=fdcc9268909f5a990576e32d11c9f054 (accessed August 25, 2007).

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, NJ: John Wiley & Sons, Inc., 2006.

Lewis, Ted G. and Rudy Darken. "Potholes and Detours in the Road to Critical Infrastructure Protection Policy." *Homeland Security Affairs* I, no. 2 (Fall 2005): 1-11, http://www.hsaj.org/pages/volume1/issue2/pdfs/1.2.1.pdf (accessed August 29, 2007).

Libicki, Martin C., Peter Chalk, and Melanie Sisson. *Exploring Terrorist Targeting Preferences*. Santa Monica, CA: Rand Corporation, 2007, http://www.rand.org/pubs/monographs/2007/RAND_MG483.pdf (accessed March 13, 2008).

Meade, Charles and Roger C. Molander. *Considering the Effects of a Catastrophic Terrorist Attack*. Santa Monica, CA: Rand Center for Terrorism Risk Management Policy, 2006, http://www.rand.org/pubs/technical_reports/2006/RAND_TR391.pdf (accessed August 26, 2007).

Moteff, John. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Washington, DC: Congressional Research Service, 2005, http://www.fas.org/sgp/crs/homesec/RL32561.pdf (accessed March 13, 2008).

———. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Washington, DC: Congressional Research Service, 2004, https://www.hsdl.org/homesec/docs/crs/nps17-100804-19.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

National Association of Insurance Commissioners, *Natural Catastrophe Risk: Creating a Comprehensive National Plan*, NAIC, (draft document, 2007).

National Science and Technology Council. *Combating Terrorism: Research Priorities in the Social, Behavioral and Economic Sciences*. Washington, DC: Executive Office of the President, Office of Science and Technology Policy, 2004, http://www.ostp.gov/nstc/html/terror.pdf (accessed August 29, 2007).

Proctor, Richard B. "Assessing the Impact of a Successful Biological Weapons Attack." *New Jersey Municipalities Magazine* 78, no. 2 (2001): 6-10.

Renn, Ortwin. *Risk Governance: Towards an Integrative Approach*. Geneva, Switzerland: International Risk Governance Council, 2006, http://www.irgc.org/irgc/IMG/projects/IRGC_WP_No_1_Risk_Governance_(reprinted_version).pdf (accessed August 26, 2007).

Ross, Robert G. "Combating Terrorism with Risk-Based Strategies." Draft Paper.

———. "Risk and Decision-Making in Homeland Security." Baltimore, MD, Society for Risk Analysis Annual Meeting, December 3-6, 2006.

Santiago, Denise and Anka Richter. "Assessment of Public Health Infrastructure to Determine Public Health Preparedness." *Homeland Security Affairs* 2, no. 3 (2006): 1-25, http://www.hsaj.org/pages/volume2/issue3/pdfs/2.3.11.pdf (accessed August 27, 2007).

Scalingi, Paula L. "Moving Beyond Critical Infrastructure to Disaster Resilience." In *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, 49-72. Arlington, VA: George Mason University, School of Law, 2007, http://cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf (accessed March 17, 2008).

Taleb, Nassim. *The Black Swan: The Impact of the Highly Improbable.* New York, NY: Random House, 2007.

Thompson, William P.Jr. *One Year Later: The Fiscal Impact of 9/11 on New York City*. New York, NY: City of New York, Office of Comptroller, 2002.

U.S. Department of Homeland Security. *National Response Framework*. Washington, DC: Department of Homeland Security, 2008, http://www.fema.gov/pdf/emergency/nrf/nrf-base.pdf (accessed March 17, 2008).

———. *FY 2007 Homeland Security Grant Program*. Washington, DC: Department of Homeland Security, 2007, https://www.hsdl.org/homesec/docs/dhs/nps22-071807-01.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

———. *National Preparedness Guidelines*. Washington, DC: Department of Homeland Security, 2007, http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf (accessed March 18, 2008).

———. *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2006, https://www.hsdl.org/homesec/docs/dhs/nps23-062906-01.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

U.S. Department of Homeland Security. Office of Inspector General. *The State of Georgia's Management of State Homeland Security Grants Awarded during Fiscal Years 2002 through 2004*. Washington, DC: Department of Homeland Security, 2008, https://www.hsdl.org/homesec/docs/dhs/nps23-021108-02.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

———. *Audit of the State of Colorado Homeland Security Grant Program*. Washington, DC: Department of Homeland Security, 2007, https://www.hsdl.org/homesec/docs/dhs/nps36-010308-02.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

———. *The State of North Carolina's Management of State Homeland Security Grants Awarded during Fiscal Years 2002 and 2003*. Washington, DC: Department of Homeland Security, 2006, https://www.hsdl.org/homesec/docs/dhs/nps22-112706-03.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

U.S. Government Accountability Office. *Homeland Security Grants: Observations on Process DHS used to Allocate Funds to Selected Urban Areas*. Washington, DC: GAO, 2007, http://www.gao.gov/new.items/d07381r.pdf (accessed August 27, 2007).

U.S. Homeland Security Council. *National Strategy for Homeland Security*. Washington, DC: The White House, 2007, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed March 17, 2008).

U.S. Senate. Committee on Homeland Security and Governmental Affairs. *Preparing for a Catastrophe: The Hurricane Pam Exercise*. Washington, DC: Government Printing Office, 2006, https://www.hsdl.org/homesec/docs/legis/nps20-011007-06.pdf&code=80382dac961e832159cc3488e6d9f002 (accessed March 13, 2008).

Willis, Henry H. "Guiding Resource Allocations Based on Terrorism Risk." *Risk Analysis* 27, no. 3 (June 2007): 597-606.

Willis, Henry H., Tom LaTourrette, Terrence K. Kelly, Scot Hickey and Samuel Neill. *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*. Santa Monica, CA: Rand Corporation, 2007, http://www.rand.org/pubs/technical_reports/2007/RAND_TR386.pdf (accessed March 13, 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Robert Bach
   Naval Postgraduate School
   Monterey, California

4. Professor Michael Chumer
   New Jersey Institute of Technology
   Newark, New Jersey

5. Governor Jon Corzine
   State of New Jersey
   Trenton, New Jersey

6. Director Richard Canas
   New Jersey Department of Homeland Security
   Trenton, New Jersey

7. Mayor James J. Kennedy
   City of Rahway
   Rahway, New Jersey